Some functions in this ebook require either the free Adobe Reader or Adobe Acrobat.

How to Configure and Secure the NetSuite AI Connector Service

ORACLE
NetSuite

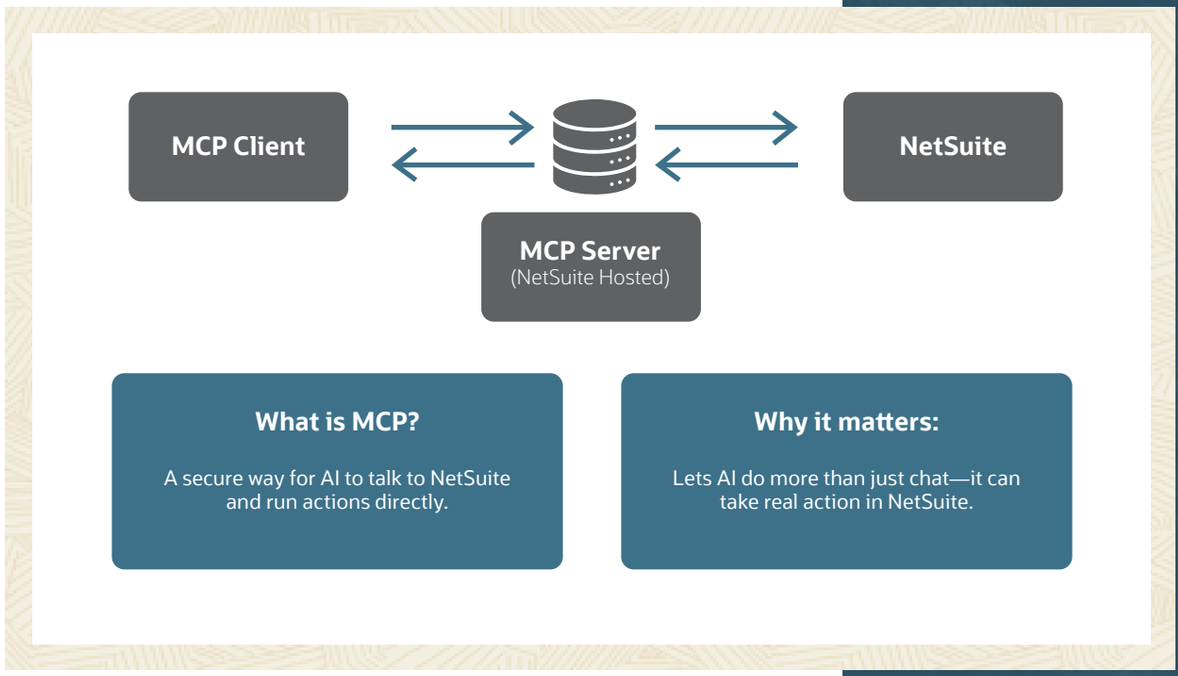
Introduction

As AI becomes part of everyday business operations, organizations need a flexible way to connect their chosen AI tools to their ERP data. The NetSuite AI Connector Service provides that bridge between NetSuite and supported AI clients such as Claude and ChatGPT using the Model Context Protocol (MCP), an open standard that enables structured, governed communication.

This ebook explains the configuration steps required to connect AI clients with the NetSuite AI Connector Service and then highlights additional practice tips for managing security and performance once setup is complete.

A connection between NetSuite and supported AI clients relies on two components that work together:

- The NetSuite AI Connector Service acts as the bridge between NetSuite and external AI clients. It controls how data and commands flow between the systems by using OAuth 2.0 authentication and applying the same user and role permissions defined in NetSuite.
- The AI client is an application that communicates with NetSuite through the connector. Supported clients include Claude, ChatGPT, and any other client that supports the MCP protocol.



How NetSuite AI Connector uses the Model Context Protocol (MCP) to connect AI clients to NetSuite.

Together, these components allow organizations to interact with NetSuite data through natural language in a controlled and auditable environment. All MCP activity is authenticated, logged, and tied to the user's assigned role, ensuring full traceability.

The following steps outline the required configuration steps for connecting AI clients to NetSuite.

Step 1: Enable Core NetSuite Features Needed to Establish a Reliable Foundation

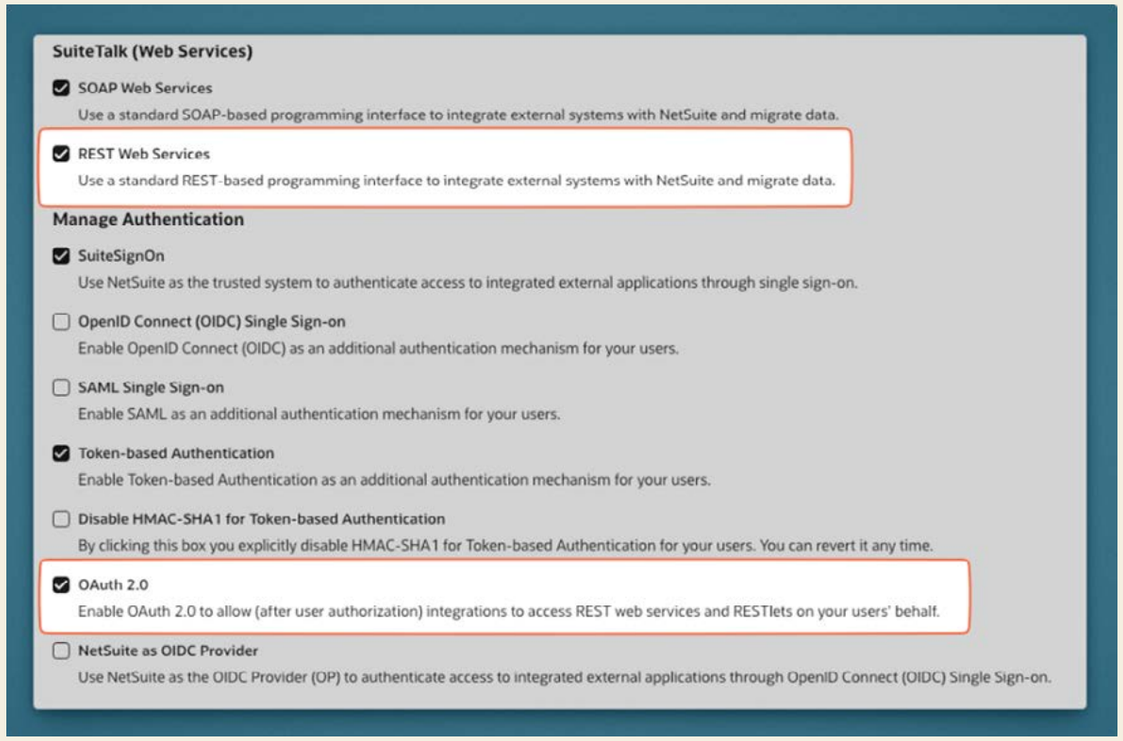
This step focuses on enabling the foundational features required for the AI Connector to enable communication with supported clients.

The NetSuite AI Connector requires specific SuiteCloud features and permissions to connect with AI clients through authenticated, role-based APIs. Turn on these settings to allow the connector to establish communication between NetSuite and supported AI clients which preserves the NetSuite user's permissions.

Practice tip: Before enabling features, review which SuiteCloud capabilities your organization already uses to avoid redundant settings or unnecessary permissions. Also check your organization's AI and data security policies to confirm compliance.

Why it matters

The AI Connector can't establish a connection unless these features are enabled. They allow NetSuite to communicate with supported AI clients through APIs that are authenticated, enforce role-based access control, and log activity through NetSuite's existing audit and usage tracking.



Enable REST Web Services and OAuth 2.0 under Setup > Company > Enable Features > SuiteCloud.

Configuration guidance

Once you confirm which features to enable, follow these configuration steps to establish a foundation for your connector.

1. Go to *Setup > Company > Enable Features.*
2. On the *SuiteCloud* subtab, enable the following:
   - Server SuiteScript
   - OAuth 2.0
   - REST Web Services (required for the MCP Standard Tools SuiteApp)
3. Click *Save.*

The features allow NetSuite to communicate with AI clients that support the Model Context Protocol. Next, install the MCP Standard Tools SuiteApp, which provides tools that allow AI clients to interact with NetSuite data.

1. Go to the *SuiteApps* tab in NetSuite.
2. In the search field, enter *MCP Standard Tools* and select the SuiteApp.
3. Click *Install* and wait for the installation to be completed.

After installation, confirm that the connector's role permissions are set correctly before any users connect an AI client. Roles must include *MCP Server Connection* and *Log in using OAuth 2.0 Access Tokens*. The Administrator role should not be used with the NetSuite AI Connector Service as it would provide unlimited access, including the ability to delete key data.

Takeaway

A properly configured environment is necessary for AI integration. Verifying these settings before connecting LLMs protects data integrity and ensures that all interactions through the connector follow NetSuite's built-in governance controls.

SuiteApps > MCP Standard Tools

Step 2: Use Role-Based Permissions to Control and Manage Connector Access

This section covers setting clear, limited access for each role to maintain access control when connecting AI clients to NetSuite.

Access control is critical when connecting AI clients to NetSuite. In this step, you're creating or editing a role that allows only designated users to access the MCP Service through the AI Connector. Limiting connector access in this way helps you to protect your sensitive data and to require that actions taken through the connection remain traceable.

Before creating or editing roles, identify which users actually need connector access and which data categories they interact with most often. This avoids giving broader permissions than necessary and keeps permission reviews simple.

Why it matters

When an AI client connects to NetSuite through the Model Context Protocol, it authenticates the NetSuite user and can perform only the actions allowed by that user's assigned role. Setting up the connector this way helps enable each request to follow your configured NetSuite permissions and governance rules.

Configuration guidance

After determining which users and roles will have connector access, follow these configuration steps to apply the correct permissions:

1. Go to *Setup > Users/Roles > Manage Roles*.
2. Edit an existing role or create a new one specifically for use of the NetSuite AI Connector.
3. Under the *Permissions > Setup* subtab, add:
   - MCP Server Connection
   - Log in using OAuth 2.0 Access Tokens
4. Assign this role only to users who will use a connected AI client.
5. Do not assign the *Administrator* role or any role with full account access to connector users as doing so will put your NetSuite data at risk.
6. Save the changes and once your preferred AI client is configured to connect through MCP, test the connection to confirm that access is limited to the intended data and actions.

Practice tip: Create separate connector roles with fewer permissions than the user's normal NetSuite role. These limited-purpose roles allow chatbot connections to run only the specific tasks or data queries needed for the workflows.

Takeaway

Connector roles should be designed with fewer permissions than a user's standard NetSuite role. Limiting access to only the tasks needed for each workflow limits what the connected AI clients can do, reducing risks of changing data or taking actions unintentionally.

Step 3: Validate and Monitor Your AI Connection to Provide Reliable Performance

This step focuses on maintaining reliability and compliance by validating operation and monitoring your AI Connector's use on an ongoing basis.

Once the connector is configured and roles are assigned, ongoing validation of operation is essential to maintain performance and reliability. The NetSuite AI Connector operates within NetSuite's standard concurrency limits, so regularly checking integration records and usage logs helps identify connection issues early and prevent disruptions.

Practice tip: Incorporate connector monitoring into your regular account review routine so issues are caught early.

Why it matters

AI connections can fail if concurrency limits are reached, if permissions change, or if the connector loses authorization. Regular validation confirms that the connector is processing requests as expected and that its access controls are still working correctly. Periodically checking will help you catch and fix issues before they interrupt daily workflows.

Configuration guidance

After confirming your connector setup and permissions, use the following checks to maintain proper operation over time:

1. Review the *Integration Record* created when the connector was first authorized.
   - Go to *Setup > Integration > Manage Integrations.*
   - Confirm that the integration is enabled and that the *NetSuite AI Connector Service* scope (the permissions granted to the connector) is active.
   - Monitor account activity to track connector usage.
   - If you experience Too Many Requests errors, adjust concurrency settings or retry the request from your AI client.
   - Consider allocating a portion of your concurrency limit specifically to the AI Connector to avoid competition with other integrations. You can view current concurrency usage under Setup > Integration > Manage Integrations to see which connections are consuming available sessions.
2. Periodically test the connection from the AI client you've chosen to use.
   - Test the connection regularly to confirm that it remains active.
   - If a connection error occurs, reauthorize the connector and retrace the steps outlined above to verify that setup and role permissions are still correct.
   - If the issue continues, recreate the connection to restore access.

Takeaway

Routine operation verification helps keep the NetSuite AI Connector reliable and secure. By checking integration records, monitoring concurrency usage, and testing connections periodically, you can detect issues early and ensure that AI interactions remain stable over time.

Note on Authentication

Authentication helps keep AI connections secure. All AI client connections use OAuth 2.0 to authorize access between NetSuite and any external system. During the first connection, users present credentials and are granted access to the connector. Each subsequent request sent through the AI client is then authenticated using those credentials, logged through NetSuite's existing auditing, and tied to that specific user's role.

This process helps you to align AI-initiated actions to follow NetSuite's existing governance model. For detailed setup instructions and additional security information, see the help topic *Connect to NetSuite AI Connector Service.*

Putting It All Together

When configured and managed properly by using the steps outlined above, the NetSuite AI Connector allows you to provide NetSuite access to trusted AI clients such as Claude and ChatGPT. By enabling the right features, setting clear role-based permissions, and monitoring connector activity, you can create a reliable foundation for using external AI tools while helping to maintain control over your NetSuite data.

Following these steps helps you to configure your connection to remain stable, scalable, and aligned with NetSuite's governance standards. With defined permissions, monitored activity, and verified access in place, teams can confidently explore new AI use cases and automation opportunities while maintaining access controls and tracking use.

ORACLE
NetSuite

Next Steps

If your organization plans to expand its AI capabilities, consider exploring how the Model Context Protocol framework supports custom tool development and orchestration across multiple business applications. For more information, see the help topic *Creating Custom Tools for the NetSuite AI Connector Service* or contact your NetSuite representative.

Supporting You Along the Way

If you want to learn more about building scalable AI integrations, check out these NetSuite resources:

- Connect to NetSuite AI Connector Service
- Associated Risks, Controls, and Mitigation Strategies
- Creating Custom Tools for the NetSuite AI Connector Service

These help topics provide detailed setup guidance, risk management recommendations, and examples of how to extend the connector using the Model Context Protocol. Together, they can help you gain a deeper understanding of how to integrate AI systems with NetSuite while maintaining access configurations and control.

Join the NetSuite Support Community

The NetSuite Support Community is an online gathering place for NetSuite professionals to share information, experiences, and advice. Ask a Support Guru for help with how-to questions or start a public discussion with the community.

Join today!

ORACLE
NetSuite

www.netsuite.com
Infonetsuite_WW@oracle.com
877-638-7848