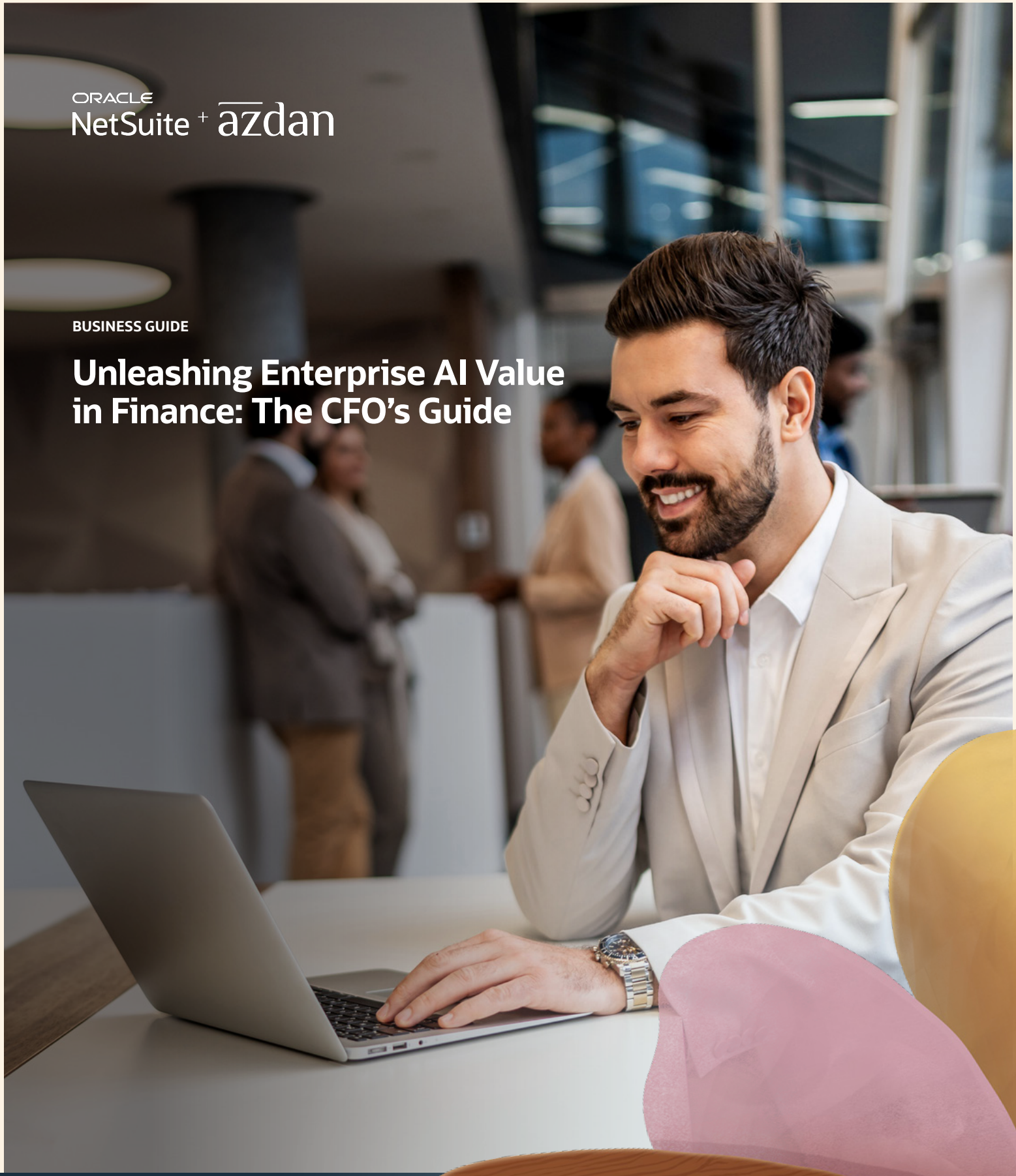
ORACLE
NetSuite + azdan

BUSINESS GUIDE

Unleashing Enterprise AI Value in Finance: The CFO's Guide



Learn more at netsuite.com

Grab a seat and enjoy.
Read Time: 13 minutes

Unleashing Enterprise AI Value in Finance: The CFO's Guide

The Protocol Moment

It's quite possible that the most important AI development of 2025 wasn't a new GenAI model… It was a protocol.

The next wave of AI value in finance won't come from bigger, smarter models. It will come from giving those models a common way to understand context, invoke tools, and act inside enterprise systems.

In November 2024, Anthropic released the Model Context Protocol (MCP) as an open standard.[1] By March, OpenAI had announced support. Google DeepMind followed in April. At its Build conference in May, Microsoft committed to migrating all Dynamics 365 agents to MCP by year's end.[2] And in August, NetSuite launched its AI Connector Service with native MCP support.[3]

That's a remarkable adoption curve for infrastructure that most business leaders have never heard of.

What Is It?

Think of MCP as the USB-C for AI.[21] It's a universal connector that lets any compatible AI assistant access any compatible data source through a single, standardized interface. Before MCP, connecting an AI tool to your ERP meant custom integration work for every combination of assistant and system. Expensive. Fragile. Ungovernable.

MCP changes that equation. AI assistants can be powerful tools, but until now they've been largely disconnected from enterprise data. The workarounds we've all used (copy-paste, manual exports, asking someone to pull a report) create friction and risk. MCP creates a governed bridge.

This is important for CFOs because it finally answers the question that's stalled AI adoption in finance: How do we give AI access to our data without losing control?

Glenn Hopper, Head of AI and Managing Director, VAi Consulting

[1] Anthropic, "Introducing the Model Context Protocol," November 2024.
[2] Microsoft, "Dynamics 365 ERP MCP Server: Adaptive & Analytics-Ready," November 2025.
[3] Enterprise Times, "NetSuite delivers AI Options with Connectors," August 2025.
[21] Anthropic, "Model Context Protocol Documentation," 2024.; Wikipedia, "Model Context Protocol."

Why Finance Has Been Right to Wait

Finance leaders aren't laggards on AI. They're appropriately cautious. The data supports this.

Gartner's September 2024 survey found 58% of finance functions now use AI, up from 37% the year before.[4] Yet research from Bain Capital Ventures shows 71% aren't using it in core finance and accounting functions. The same study found 94% of CFOs believe AI can strongly benefit at least one finance activity.[5, 20]

That gap between belief and action reflects real concerns.

Top of the list: Data Quality. Gartner identifies data quality as the primary obstacle to generative AI adoption in finance—and with good reason.[4] Only 11% of organizations have fully implemented data governance capabilities.[6] Finance leaders know their data is frequently fragmented across systems, inconsistently formatted, and often incomplete. AI outputs are only as reliable as the inputs.

There is also a huge skills gap around AI. Deloitte's Q1 2025 CFO survey found 45% cite lack of skilled talent as a primary workforce issue.[7] The accounting profession itself faces headwinds: 340,000 fewer accountants work in the field compared to five years ago.[8] The conundrum is that finance teams need AI that reduces complexity. They don't need tools requiring additional technical expertise to deploy.

Then there's uncertainty around governance. Only 32% of organizations have formal AI governance programs in place. Roughly 63% haven't defined formal risk appetite

[4] Gartner, "Gartner Survey Shows 58% of Finance Functions Using AI in 2024," September 2024.
[5] Bain Capital Ventures, "AI and the Office of the CFO in 2025," 2025.
[6] Ideas2IT, "AI Governance in Finance: Key Strategies and Challenges," 2024.
[7] The CFO, "How are North American CFOs dealing with the growing talent shortage," April 2025.
[8] CFO Dive, "Accounting talent shortage eases as layoff fears creep up," 2024.
[20] BCG, "AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value," October 2024.

or frameworks for AI use.[9] Without clear policies, individual adoption decisions become judgment calls. That's exactly the opposite of how finance functions typically operate.

These concerns are all warranted. The question then becomes whether protocol-based access changes the calculus.

The good news is that it does!

What MCP Actually Solves

Here's the technical reality: Before MCP, developers faced what they call the "N×M integration problem." Connecting multiple AI applications to multiple data sources required custom code for each combination. A company using three AI tools and five data systems needed fifteen separate integrations. Each one had to be built, maintained, and secured independently.

This protocol collapses that complexity. MCP Servers (like NetSuite's) declare exactly what they expose: specific queries, searches, and record types. AI clients discover these capabilities when they connect. Users authorize what the AI can access based on their existing permissions. The AI can only see and do what the server explicitly permits.

This architecture matters for governance in ways that embedded AI features can't match.

It creates an enforceable boundary between what AI requests and what it receives. It inherits existing role-based security rather than requiring parallel permission structures. It enables audit trails for every AI-initiated query. And it supports human-in-the-loop approval for actions, meaning you can require sign-off before the AI actually does anything.

The key insight here is that MCP doesn't require finance teams to just "trust AI."

It lets them extend their existing trust model to AI interactions. The roles, permissions, and access controls you've already built? They also govern the AI.

Where to Apply MCP

What does governed AI access actually look like in daily operations?

[9] Corporate Compliance Insights, "AI Adoption Presses on Even as Controls Lag," December 2024.

Invoice Lookup and Payment Status

A customer calls to ask about an invoice. Today, an analyst navigates to their ERP, searches for the invoice, checks payment history, reviews the communications log, and compiles an answer. Three to five minutes per inquiry.

With NetSuite's MCP capabilities, the analyst could ask an AI assistant: "What's the status on invoice #12345 for ABC Corp?" The AI queries NetSuite, returns the amount, due date, payment history, and last communication date. It formats the response with context: "Invoice is 15 days overdue. Last payment reminder sent 7 days ago. Recommend follow-up call."

Resolution drops from minutes to seconds. More importantly, the AI provides an actionable recommendation rather than raw data.

AR Aging and Collections Prioritization

Today's process: The weekly aging report is generated, exported to Excel, and manually analyzed for patterns. Prioritization is based on dollar amount or days overdue.

With MCP, the AI queries aging data directly, applies pattern recognition based on customer payment history, and generates a prioritized action list weighted by likelihood of collection and impact on cash flow. Organizations using AI-enhanced AR management report DSO reductions from 45 to 30 days. Overdue percentages drop from 20% to 15%.[10]

The intelligence layer transforms static reporting into dynamic decision support.

Budget vs. Actual Variance Analysis

FP&A analysts know the routine. They pull the budget-to-actuals report, build variance analysis in a spreadsheet, then investigate material variances, manually digging through the G/L and other reports, and prepare a narrative for leadership.

With MCP, the analyst asks: "Why is COGS over budget this month when revenue was down?" The AI queries actuals, compares to budget, identifies specific drivers (raw material price increases, freight surcharges, and volume changes), and provides a structured breakdown. It could even include recommendations based on historical ROI data from similar situations.

McKinsey documents finance professionals spending 20 to 30% less time on data compilation in these scenarios. That time gets redirected to analysis and decision-making.[11]

Vendor Payment Compliance

AP processes invoices against PO terms, but contract nuances often slip through in high-volume environments. Early payment discounts, volume rebates, and pricing tiers can be a nightmare to track, but these details matter when determining whether you're paying the right amount.

With MCP, the AI can validate invoices against contract terms before payment. It flags discrepancies, identifies missed discounts, and routes exceptions to appropriate approvers.

The financial impact here is substantial. A McKinsey case study found compliance checking identified contract leakage equal to roughly 4% of total spend. For a company with $1 billion in nominal spend, that's $40 million in recurring margin improvement.[12]

Governance Without Gridlock

To be clear, as of the time of this writing, no authoritative AI ethics framework exists yet for financial systems.

The PCAOB's July 2024 spotlight acknowledged that GenAI integration in audits is "in its early stages, but rapidly evolving." The guidance emphasized "the importance of the auditability of both the underlying source data and GenAI-created content."[13] So, while regulators are clearly watching the space, they haven't yet prescribed specific requirements.

This creates both risk and opportunity for organizations establishing early practices.

[10] Growfin, AR Automation benchmarks, 2024.
[11] McKinsey & Company, Finance AI productivity research, 2025.
[12] McKinsey & Company, Contract compliance case study, 2025.
[13] PCAOB Spotlight, "Staff Update on the Use of Generative Artificial Intelligence," July 2024.

SOX implications are straightforward in principle: When AI-driven processes support financial reporting, they become subject to Section 404 requirements. That means documenting AI logic for accuracy and bias, implementing AI-specific IT general controls covering access management and change control, and ensuring human oversight mechanisms for AI outputs that affect financial statements.

SOC 2 presents a different challenge. The Trust Services Criteria weren't designed for AI-specific risks, so in this area processing integrity becomes particularly important as auditors will require evidence that models are explainable and that outputs meet quality control standards. Organizations can supplement SOC 2 examinations with testing of ISO 42001's 38 AI-specific controls, which cover responsible use, lifecycle management, and testing techniques.[14]

For any MCP implementation, audit trails should capture four things:[15]

1. Every AI-initiated query with timestamp, user context, and data accessed.
2. Permission scope validation recording what the AI requested versus what was granted.
3. Action attribution linking AI recommendations to resulting business actions.
4. Human-in-the-loop documentation recording when users reviewed, modified, or approved AI outputs.

The Center for Audit Quality advises audit committees to develop "foundational understanding of how GenAI works and the benefits and risks."[16] That's capability-building for finance leadership, and it starts now.

First movers don't just adapt to governance standards. They help define them.

[14] Schellman, "How to Incorporate AI Controls into Your SOC 2 Examination," 2024.
[15] Aembit, "Auditing MCP Server Access: Complete Security Guide," 2025.
[16] Center for Audit Quality, AI governance guidance for audit committees, 2024.

How NetSuite Approached This

Design decisions reveal priorities, and NetSuite's MCP implementation shows exactly how they're thinking about this shift.

The key decision is that AI access flows through the same role-based permissions already in place so there's no parallel security model to maintain. Whatever the user's role can see, the AI can see. Nothing more. Brian Chess, SVP of Technology and AI at Oracle NetSuite, put it simply: "We use all of the things that people are used to in terms of being able to control their integrations."[17]

The explicit restrictions matter too. Administrator roles can't access MCP tools. Neither can roles with full NetSuite permissions. Elevated privilege scripts cannot be invoked via MCP. Tools cannot make external HTTP requests. And session isolation prevents one AI connection from seeing data requested by another.[18]

The philosophy here is to be "secure by default." AI capabilities are limited to what's appropriate for standard business users.

A brief note on the competitive landscape: Microsoft has made a similar MCP commitment for Dynamics 365, with full migration planned by December 2025.[2] SAP and Workday have taken different approaches, emphasizing embedded AI through Joule and Illuminate respectively.[19] Those platforms offer deeper out-of-box capabilities within their ecosystems. Protocol-based approaches offer more flexibility to swap AI providers as the market evolves.

Different architectures for different priorities. Finance leaders should understand the tradeoffs.

Starting: The 90-Day Pilot Framework

Effective MCP pilots follow three phases:

Phase 1: Foundation (Days 1-30)

Select a single high-impact, low-risk use case. One. The temptation to prove value across multiple workflows simultaneously leads to diffuse effort and unclear results.

[17] Diginomica, "With NetSuite's MCP integration, you can plug your enterprise data and actions into any LLM-based AI agent," 2025.
[18] Oracle NetSuite, "What is the NetSuite AI Connector Service?" 2025.
[19] SAP, "Joule Agents: How SAP Uniquely Delivers AI Agents That Truly Mean Business," February 2025.

AP invoice processing and data reconciliation make ideal starting points. They have clear baselines, outcomes are measurable, and write operations are limited, which reduces risk.

Secure a VP or CFO-level sponsor. This will help remove barriers down the line. Get a signed green-light document confirming the problem statement, KPIs, cost ceiling, and timeline. Without executive sponsorship, pilots stall when they hit the inevitable friction points.

Phase 2: Pilot Execution (Days 31-60)

Launch with three to five power users. Don't just choose the AI evangelists. Great to have them on the team, but it's important to round out the group with a couple of skeptics. You want people who'll use the tools seriously and report honestly on what works.

Hold weekly operations meetings to review latency, accuracy, and adoption statistics. Document edge cases rigorously, as they'll inform your scale decisions later.

Monthly finance check-ins translate KPI changes to dollar terms. This is essential for building executive support. "Reduced processing time by 30%" is good. "Saved 120 hours per month, equivalent to $15,000 in labor costs" is better.

Phase 3: Evaluation and Scale Decision (Days 61-90)

Formalize SOPs for new workflows. The pilot proved the concept; now document it for handoff.

Prepare board-ready results documentation. Make an explicit go/no-go decision. If you proceed, define the expansion roadmap with specific use cases and timelines.

- **Target metrics to track:** Hours saved per cycle should show 20-40% reduction. Touchless processing rate should hit 70% or higher for appropriate transactions. Error and rework rates should drop by 50% or more.
- **Budget guidance:** Cap first pilots at $25,000 to $50,000. Use non-production data initially where possible. Expect 12-18 months to full ROI realization, but visible wins should emerge within this 90-day window. If they don't, something's wrong with the use case selection or implementation approach.

Technical Guide for NetSuite Administrators

Implementing the MCP Standard Tools SuiteApp

What You're Actually Setting Up

AI implementations are like traditional software integrations. There's no middleware to configure or custom code to write. You're configuring NetSuite to expose specific capabilities through a standardized protocol, then connecting AI clients to that endpoint.

Think of it as creating a controlled API surface that AI assistants can discover and use. The server declares what's available, and the MCP client discovers those capabilities at runtime. User permissions govern what data flows through.

This guide covers architecture (enough to make good decisions), prerequisites, role configuration, available tools, security guardrails, OAuth setup, migration notes for Sample Tools users, and common troubleshooting scenarios.

It assumes working knowledge of NetSuite administration, familiarity with role-based permissions, and basic understanding of OAuth authentication.

Architecture in Five Minutes

You don't need deep architectural knowledge to implement MCP. But understanding the basics helps you make better configuration decisions.

The system follows a client-host-server model:

- The MCP Server (NetSuite's AI Connector Service) exposes tools, handles requests, and enforces permissions.
- The MCP Client (Claude, ChatGPT, or another compatible assistant) discovers available tools, sends requests, and displays results.

Communication happens via JSON-RPC 2.0 over standard HTTPS.

The client connects to the server endpoint, which kicks off capability discovery. The server returns a list of available tools based on the authenticated user's role. Importantly, the client can only invoke tools the server has declared. Each invocation includes user context for permission validation.

This matters for your configuration work because the role you create defines the ceiling of AI capabilities. Tools the role can't access won't appear to the AI client at all. The role is your primary control mechanism.

One concept to internalize: the AI doesn't have its own permissions. It *inherits* the permissions of the user whose credentials authenticate the connection. Configure the role carefully. Everything flows from there.

Prerequisites Checklist

NetSuite environment requirements

Three features need to be enabled. Navigate to Setup > Company > Enable Features > SuiteCloud for all of them.

Server SuiteScript must be on. REST web services must be on. OAuth 2.0 must be enabled under Manage Authentication in the same SuiteCloud section.

You'll need administrator access for initial setup, the ability to create custom roles, and the ability to install SuiteApps from the marketplace.

AI client requirements

Not all subscription tiers support MCP connections. For Claude, you need Pro, Team, or Enterprise. For ChatGPT, you need Plus with Developer mode enabled or Team/ Enterprise tiers. Other AI clients vary. Check their documentation for MCP support.

On the client side, you'll need the ability to add custom MCP server connections and a place to securely enter OAuth credentials.

Network considerations

The AI client needs outbound connectivity to your NetSuite endpoint. Verify no firewall rules block the MCP endpoint URL. Standard HTTPS/TLS requirements apply.

Installing the MCP Standard Tools SuiteApp

Navigate to the SuiteApp Marketplace and search for "MCP Standard Tools." Verify the publisher is Oracle/NetSuite before installing.

Installation follows the standard SuiteApp workflow. Accept terms and permissions. The process typically completes within a few minutes.

After installation, confirm the SuiteApp appears in your installed applications list. Check system logs for any installation errors. Verify the MCP tools appear in expected locations.

One important distinction: MCP Standard Tools is the production version. (MCP Sample Tools was the original beta release.) If you have Sample Tools installed, you'll need to migrate to the new tool (covered in the migration section below).

Note, the SuiteApp will update automatically with NetSuite releases. Check release notes for new tools or changed capabilities. Where possible, test updates in sandbox before they hit production.

Role Configuration

This is the most important section in this guide. The role you create is your primary governance mechanism. Every permission decision here flows through to what AI assistants can access.

Creating the dedicated MCP role

Navigate to Setup > Users/Roles > Manage Roles. Create a new role. Don't modify existing operational roles for MCP use. Keep it separate.

Name the role clearly. Something like "MCP AI Access - Finance" or "MCP AI Access - AR Team" makes the purpose obvious to anyone reviewing your role structure later.

Permission categories to configure

Work through each category deliberately.

Transactions: Which transaction types can be queried? Created? Modified? Be specific. Invoice read access, for example, is different from invoice creation.

- Reports: Which reports can be executed through the AI connection? Start with the reports your pilot use cases require.
- Lists: Which record types should be visible? Customers, vendors, items, and employees? Each one is a decision.
- Custom Records: If you have custom objects the AI should access, grant them explicitly.

The principle of least privilege

Start with minimal permissions, and add only when use cases require them. Document why each permission was granted. It's good practice to review quarterly and remove anything that's gone unused.

This approach takes more time upfront, but it saves you from explaining to auditors why your AI connection had access to compensation data when your use case was invoice queries.

Restrictions that apply regardless of your configuration

Some guardrails are system-enforced. You can't override them.

- Administrator roles can't access MCP tools.
- Full permission roles can't access MCP tools.
- Elevated privilege scripts can't be invoked through MCP.
- External HTTP requests are blocked.

These restrictions exist by design, and built to limit AI capabilities to what's appropriate for standard business users.

Subsidiary and multi-entity considerations

If you operate across subsidiaries, role restrictions by subsidiary apply to MCP access. Cross-subsidiary queries follow standard NetSuite rules. Pro tip: Consider separate MCP roles for different business units if data separation matters for your organization.

Testing the role before connecting AI

Assign the role to a test user. Log in as that user. Manually verify the expected access levels. Can you see the records you intended? Are restricted records actually hidden?

Document the baseline of what the role can see. This documentation becomes valuable when you're troubleshooting unexpected AI behavior later.

Common configuration mistakes

- Granting too many permissions initially. The temptation is to add everything and pare back. Resist it.
- Using an existing operational role instead of a dedicated MCP role. This creates permission creep and audit complications.
- Forgetting to restrict sensitive record types. Compensation data, M&A information, and board materials. If it shouldn't flow to an AI assistant, verify the role can't see it.
- Not testing the role as an actual user before AI connection. The role might look right in configuration. Test it in practice.

Available Tools Reference

The MCP Standard Tools SuiteApp exposes 9-13 tools depending on role permissions. They fall into four categories.

1. Record Tools. Create Record lets you create new records (customers, vendors, and transactions) via the REST API. Retrieve Record fetches record details by internal ID or external ID. Update Record modifies existing record fields. Search Records queries records with filters and criteria.

   These tools are governed by transaction and list permissions in your role configuration.

2. Report Tools. List Reports returns available reports based on role access. Execute Report runs a report and returns results.

   Governed by report permissions in your role configuration.

3. Saved Search Tools. List Saved Searches returns saved searches visible to the role. Run Saved Search executes a search and returns results.

   Governed by saved search permissions. The AI can access public searches plus searches owned by or shared with the role.

4. SuiteQL Tools. Execute SuiteQL runs custom queries using NetSuite's SQL-like syntax.

   Governed by record-level permissions. The role's access to specific tables and fields determines what's queryable.

Known limitations to communicate to your users

Standard financial reports like P&L and balance sheet require custom configuration to access via MCP. NetSuite Analytics Warehouse isn't accessible through the protocol. Neither is Enterprise Performance Management.

Saved searches with very large result sets may timeout. Complex SuiteQL queries can hit performance constraints.

What to tell finance users in plain terms

The AI can query data and run reports you already have access to. It cannot see anything your role can't see. It cannot access admin functions, run scripts, or connect to external systems.

Security Model and Guardrails

System-enforced restrictions

These cannot be overridden through configuration. They're built into the platform.

On the role side: Administrator roles are blocked from MCP access. Full permission roles are blocked. The AI inherits the authenticated user's permission ceiling and cannot exceed it.

On the capability side: No elevated privilege script invocation. No external HTTP requests from tools. No direct database access. All queries flow through NetSuite's data layer.

On the session side: Connections are isolated. One AI client's session cannot see another's requests or data. Session tokens expire according to your OAuth configuration.

Authentication model
The system uses OAuth 2.1 with PKCE. It supports enterprise identity providers. Token refresh is handled by the client. Rotate credentials quarterly at minimum.

Audit logging
All MCP tool invocations are logged in NetSuite system logs. Logs capture timestamp, user context, tool invoked, and parameters passed.

Retain logs according to your standard retention policy. Consider extended retention for queries touching SOX-relevant data.

What MCP doesn't do
MCP governs NetSuite access. It doesn't provide cross-system data governance. Content filtering of AI responses is the AI provider's responsibility. And the protocol doesn't prevent prompt injection at the input layer. If that's a concern, implement input validation at the client layer.

OAuth Credential Setup and Client Connection
Creating the integration record
Navigate to Setup > Integration > Manage Integrations > New.

Name the integration clearly. Something like "Claude MCP Connection - Finance Team" identifies both the client and the user group.

Enable OAuth 2.0. Select the appropriate scope, typically REST Web Services. Save the record and securely store the consumer key and consumer secret. You won't be able to retrieve the secret later.

Generating access tokens
Follow NetSuite's standard OAuth 2.0 token generation flow. Use the MCP-specific role you created, not an admin account.

Store tokens in a secure secrets manager. Not in plaintext. Not in shared documents. Not in email.

Configuring the AI client
For Claude: Access MCP settings in the Claude interface. Add a new server connection. Enter your NetSuite MCP endpoint URL and provide the OAuth credentials. Test the connection before relying on it.

For ChatGPT: Enable Developer mode if you're on Plus. Navigate to MCP configuration. Add the server with endpoint and credentials. Verify the connection.

Testing the connection
Start simple. A basic read query like "List my recent invoices" confirms the pipe is working.

Verify results match expected data for the authenticated role. Check NetSuite system logs for corresponding MCP activity. You should see the tool invocation logged with appropriate user context.

Document your successful connection configuration. You'll reference it when setting up additional connections or troubleshooting issues.

Credential management practices
Rotate credentials quarterly. Revoke immediately if you suspect compromise. Use separate credentials for production and sandbox environments. Never share credentials across users or teams.

Migration From Sample Tools
The MCP Sample Tools SuiteApp will stop functioning in December 2025.

This affects organizations that deployed MCP during the beta period using the original Sample Tools SuiteApp. If you implemented MCP before mid-2025, check which SuiteApp you're running.

Migration steps
Install the MCP Standard Tools SuiteApp. Review your role configurations, as the permission model may have changed slightly. Update OAuth credentials if required.

Test all workflows currently in production. Don't assume they'll work identically. Some tool names differ slightly. Some parameter formats were updated. The Standard version includes additional tools.

Only uninstall Sample Tools after you've verified Standard Tools is working correctly.

Recommended timeline
Complete migration by the end of Q3 2025. That gives you a buffer before the December deprecation date. Rushing migrations in November creates unnecessary risk.

Troubleshooting Common Issues

Connection failures

Verify OAuth credentials are valid and haven't expired. Confirm the REST Web Services feature is enabled. Check network connectivity to the NetSuite endpoint. Review the integration record status. Is it active or was it deactivated?

Permission errors

The user role may lack permission for the requested record type or report. Check your role configuration against the specific query that failed.

The role might be administrator or full-permission, both of which are blocked by design.

For saved search errors, verify the search is shared with the MCP role or is set to public.

Records restricted by subsidiary won't be accessible if the role can't access that subsidiary.

Tool discovery issues

If the AI client can't see expected tools, verify the SuiteApp installed successfully. Check that the role has the required MCP permissions. Confirm all feature flags are enabled in the NetSuite account.

Performance problems

Saved searches returning too many records will slow down or timeout. Add filters to reduce result sets.

Complex SuiteQL queries may need simplification or pagination.

If you're hitting rate limits, space out your requests. The system has built-in throttling to protect performance.

Where to get help

Oracle NetSuite documentation is the primary source. The NetSuite community forums have active MCP discussions. Your NetSuite administrator or implementation partner can help with organization-specific issues. For production-blocking problems, open a case with Oracle support.

Go-Live Checklist

Quick reference for implementation:

- Features enabled: Server SuiteScript, REST Web Services, and OAuth 2.0
- MCP Standard Tools SuiteApp installed and verified
- Dedicated MCP role created with documented permissions
- Role tested manually by logging in as assigned user
- OAuth integration record created with credentials securely stored
- AI client configured with endpoint and credentials
- Connection tested with simple read query
- Audit logging verified in NetSuite system logs
- Internal documentation completed for handoff and support

ORACLE
NetSuite

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

facebook.com/netsuite

twitter.com/netsuite

linkedin.com/company/netsuite

instagram.com/oraclenetsuite