SSO Configuration Guide

Document ID: IT-ACC-010 **Last Updated:** March 2024 **Owner:** IT Security **Applies To:** IT Administrators, Application Owners

---

Overview

NovaTech uses Single Sign-On (SSO) to provide secure, centralized authentication for all enterprise applications. This guide covers SSO configuration for administrators integrating applications with our identity provider.

Identity Provider

Primary IdP: Okta

NovaTech uses Okta as our primary identity provider: **- Okta URL:** novatech.okta.com **- Admin console:** novatech-admin.okta.com

Supported Protocols

Protocol	Use Case	Preferred
SAML 2.0	Enterprise applications	Yes
OIDC	Modern web apps, APIs	Yes
LDAP	Legacy applications	No (deprecated)
WS-Federation	Microsoft applications	Sometimes

SAML Configuration

NovaTech IdP Metadata

Metadata URL: `https://novatech.okta.com/app/metadata`

Field	Value
Entity ID	`https://novatech.okta.com`
SSO URL	`https://novatech.okta.com/app/sso/saml`
SLO URL	`https://novatech.okta.com/app/sso/logout`
Certificate	Available in admin console

Adding a SAML Application

1. **In Okta Admin:**
   - Go to Applications → Add Application
   - Search for app or choose SAML template
   - Configure SP settings
2. **Required SP Information:**
   - ACS URL (Assertion Consumer Service)
   - Entity ID (SP Entity ID)
   - Name ID format (usually email)
   - Attribute mappings
3. **Configure Attributes:**

```xml
<saml:Attribute Name="email">
  <saml:AttributeValue>user.email</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="firstName">
  <saml:AttributeValue>user.firstName</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="lastName">
  <saml:AttributeValue>user.lastName</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="groups">
  <saml:AttributeValue>user.groups</saml:AttributeValue>
</saml:Attribute>
```

4. **Assign Users/Groups:**
   - Assign to appropriate groups
   - Test with pilot users first

SAML Attribute Mappings

Application Field	Okta Attribute	Format
Email	user.email	email
First Name	user.firstName	string
Last Name	user.lastName	string
Display Name	user.displayName	string
Username	user.login	email
Groups	user.groups	array
Department	user.department	string
Title	user.title	string

OIDC Configuration

NovaTech OIDC Settings

Discovery URL: `https://novatech.okta.com/.well-known/openid-configuration`

Endpoint	URL
Authorization	`https://novatech.okta.com/oauth2/v1/authorize`
Token	`https://novatech.okta.com/oauth2/v1/token`
UserInfo	`https://novatech.okta.com/oauth2/v1/userinfo`
JWKS	`https://novatech.okta.com/oauth2/v1/keys`

Adding an OIDC Application

1. **In Okta Admin:**
   - Go to Applications → Add Application
   - Choose OIDC - Web Application
   - Configure OAuth settings
2. **Configuration Options:**

```
client_id: [generated]
client_secret: [generated]
grant_types:
  - authorization_code
  - refresh_token
redirect_uris:
  - https://app.example.com/callback
post_logout_redirect_uris:
```

```yaml
  - https://app.example.com/logout
scopes:
  - openid
  - profile
  - email
  - groups
```

3. **Scopes Available:**

Scope	Claims Returned
openid	sub
profile	name, given_name, family_name
email	email, email_verified
groups	groups
offline_access	refresh_token

OIDC Token Configuration

```json
{
  "sub": "user@novatech.com",
  "name": "John Doe",
  "email": "john.doe@novatech.com",
  "groups": ["engineering", "all-employees"],
  "iss": "https://novatech.okta.com",
  "aud": "client_id",
  "iat": 1234567890,
  "exp": 1234571490
}
```

Application Integration Guides

Google Workspace

Protocol: SAML 2.0

1. Okta has pre-configured Google Workspace integration
2. Add Google Workspace from Okta application catalog
3. Configure domain verification
4. Enable for all users

Salesforce

Protocol: SAML 2.0

Configuration: - ACS URL: `https://novatech.my.salesforce.com` - Entity ID: `https://novatech.my.salesforce.com` - Name ID: Email address

Slack

Protocol: SAML 2.0

1. Add Slack from Okta catalog
2. Configure in Slack admin (Enterprise Grid)
3. Enable SSO enforcement

GitHub

Protocol: SAML 2.0

Configuration: - Available for GitHub Enterprise - Configure in GitHub org settings - Map Okta groups to GitHub teams

AWS

Protocol: SAML 2.0

1. Create AWS identity provider
2. Configure IAM roles for SAML
3. Map Okta groups to AWS roles

```
attribute_mappings:
  https://aws.amazon.com/SAML/Attributes/Role: appuser.awsRoles
  https://aws.amazon.com/SAML/Attributes/RoleSessionName: user.email
  https://aws.amazon.com/SAML/Attributes/SessionDuration: 3600
```

Custom Applications

For custom applications, provide:

SAML:

```
idp_metadata_url: https://novatech.okta.com/app/metadata
idp_sso_url: https://novatech.okta.com/app/sso/saml
idp_certificate: [Download from Okta]
name_id_format: emailAddress
```

OIDC:

```
discovery_url: https://novatech.okta.com/.well-known/openid-configuration
client_id: [Request from IT]
client_secret: [Secure storage]
scopes: openid profile email groups
```

Group Management

Standard Groups

Group	Description	Auto-membership
all-employees	All active employees	Yes (Workday sync)
engineering	Engineering department	Yes (Workday sync)
sales	Sales department	Yes (Workday sync)
contractors	Contractors	Manual

Application Access Groups

Group	Applications
app-github	GitHub
app-salesforce	Salesforce
app-aws	AWS Console
app-datadog	Datadog

Group Rules

```
IF user.department == "Engineering"
THEN add to groups: engineering, app-github, app-aws
```

Security Settings

Authentication Policies

Policy	Settings
Standard	Password + Okta Verify
Sensitive Apps	Password + Hardware key
External Access	Password + Okta Verify + Device trust

Session Settings

Setting	Value
Session lifetime	12 hours
Idle timeout	2 hours
Max concurrent sessions	5
Re-authentication for sensitive	Yes

MFA Requirements

All applications require MFA: - Okta Verify (push) - WebAuthn (hardware key) - SMS backup (limited)

Troubleshooting

Common Issues

"Invalid SAML response" - Check clock sync (±5 minutes) - Verify ACS URL matches exactly - Check certificate expiration

"User not assigned" - Verify user is assigned to app in Okta - Check group membership - Review assignment rules

"Invalid redirect URI" - URI must match exactly (OIDC) - Check for trailing slashes - Verify HTTPS

"Token expired" - Check token lifetime configuration - Verify server time - Review refresh token setup

Debug Tools

```
# Decode SAML response
base64 -d saml_response.txt | xmllint --format -
```

```
# Decode JWT token
jwt decode $TOKEN

# Test OIDC discovery
curl https://novatech.okta.com/.well-known/openid-configuration
```

Support Escalation

1. Check Okta system status
2. Review application logs
3. Enable debug logging
4. Contact IT Security: it-security@novatech.com

Requesting New Integrations

Process

1. Submit IT request at it.novatech.com
2. Provide:
    - Application name and vendor
    - Protocol preference (SAML/OIDC)
    - SP metadata or configuration
    - User access requirements
3. Security review (if new vendor)
4. IT configures integration
5. Test with pilot group
6. Roll out to users

Timeline

Request Type	Timeline
Catalog app (existing)	1-2 days
Custom app (standard)	3-5 days
Custom app (complex)	1-2 weeks
New vendor (security review)	2-4 weeks

Best Practices

For Administrators

1. Use groups for access control (not individual users)
2. Enable provisioning when available
3. Implement appropriate session lifetimes
4. Regular access reviews

For Developers

1. Use OIDC for new applications
2. Never store credentials - use SSO
3. Implement proper token validation
4. Handle token refresh gracefully

Security

1. Always require MFA
2. Use appropriate authentication policies
3. Monitor authentication events
4. Regular certificate rotation

Related Documents

- Account Provisioning (IT-ACC-005)
- MFA Policy (IT-SEC-012)
- Access Control Policy (IT-SEC-010)
- Application Security Standards (IT-SEC-035)

Contact

- **IT Security:** it-security@novatech.com
- **SSO Issues:** sso-support@novatech.com
- **New Integrations:** it@novatech.com

Review Cycle: Annual Next Review: March 2025