SurePassID

InstallationManager- Administrator Guide

Overview

The **InstallationManager** (SystemUpdateAppCore) is a comprehensive Windows desktop application designed for system administrators to manage SurePassID Authentication Server installations. This tool provides a centralized interface for performing upgrades, applying maintenance releases, managing configurations, and rotating encryption keys.

Purpose

The InstallationManager serves as the primary administrative tool for: - **In-Place Upgrades**: Upgrading existing installations to newer versions - **Configuration Synchronization**: Syncing configurations between installations - **Maintenance Releases**: Applying patches and updates to current installations - **Key Rotation**: Rotating system encryption keys for enhanced security - **Configuration Viewing**: Inspecting current system configurations

System Requirements

Minimum Requirements

- **Operating System**: Windows 10 (1809) or Windows Server 2016 or later
- **Framework**: .NET 8.0 Runtime (Desktop)
- **Privileges**: Local Administrator rights
- **Memory**: 512 MB RAM minimum
- **Disk Space**: 100 MB free space for application and temporary files

Recommended Requirements

- **Operating System**: Windows 11 or Windows Server 2022
- **Memory**: 2 GB RAM or more
- **Disk Space**: 1 GB free space for backups and logs

Installation & Deployment

Standard Installation

The InstallationManager is typically deployed alongside the SurePassID Authentication Server installation package. The executable is named:

InstallationManager.exe

Standalone Deployment

For standalone deployment, ensure the following files are present: - InstallationManager.exe (main executable) - ConfigurationManagementLib.dll (configuration library) - Supporting dependencies (.NET 8.0 runtime libraries)

Command-Line Deployment

The tool can be launched with a production folder path as a parameter:

InstallationManager.exe "C:\Program Files\SurePassID\MfaServer"

Administrative Tasks

Task 1: Planning an In-Place Upgrade

Pre-Upgrade Checklist

1. **Backup Database**: Create a complete backup of the SurePassID database
2. **Document Current State**: Note current version and configuration settings
3. **Schedule Downtime**: Plan maintenance window with users
4. **Review Release Notes**: Check for breaking changes or special considerations
5. **Test in Non-Production**: If possible, test the upgrade in a development/staging environment

Upgrade Package Preparation

1. Obtain the official SurePassID upgrade package
2. Extract to a known location (e.g., C:\Temp\SurePassID_Upgrade)
3. Verify package contents include web.config template and binaries

Risk Mitigation

- **Automatic Backup**: The tool creates timestamped backups before any modifications

- **Preview Mode**: Use preview mode to see what changes will occur without applying them
- **Rollback Plan**: Keep the backup location accessible for manual rollback if needed

Task 2: Applying Maintenance Releases

Maintenance releases are lower-risk updates that typically include: - Bug fixes - Security patches - Minor feature enhancements - No database schema changes

Maintenance Release Process

1. **Obtain Package**: Download the maintenance release package (ZIP or folder)
2. **Verify Production Folder**: Confirm the target installation folder
3. **Select Operation**: Choose “Install maintenance release” from the Operations menu
4. **Specify Package**: Browse to the maintenance package location
5. **Enable Preview (Optional)**: Check the preview box to review changes first
6. **Execute**: Click “Start” to apply the maintenance release

What Happens During Maintenance Release

- Files in the production folder are backed up
- New binaries are copied from the maintenance package
- Configuration files (web.config) are preserved
- No database migrations are performed
- Application restarts may be required

Task 3: Managing Configuration Synchronization

When running multiple instances or performing side-by-side installations:

Configuration Sync Scenarios

- **Blue-Green Deployments**: Sync configuration from blue to green environment
- **Load-Balanced Instances**: Ensure consistent configuration across instances
- **Disaster Recovery**: Replicate configuration to DR site

Synchronization Process

1. Identify the **source** (current production) folder

2. Identify the **target** (new installation) folder
3. Select “Sync web.config to new installation” operation
4. Specify both folders
5. Review the configuration viewer to verify settings
6. Execute the synchronization

Task 4: Encryption Key Rotation

Regular key rotation is a security best practice and may be required for compliance.

Key Rotation Schedule Recommendations

- **Standard Environment**: Every 12-18 months
- **High-Security Environment**: Every 6-12 months
- **After Security Incident**: Immediately
- **Compliance-Driven**: As per organizational policy

Key Rotation Prerequisites

1. **Full Database Backup**: Must be recent and verified
2. **System Downtime**: Users must be logged out
3. **Sufficient Time**: Allow 30-60 minutes for large databases
4. **Administrator Access**: SQL Server and application permissions

Key Rotation Procedure

1. Notify all users of upcoming downtime
2. Stop the application services/IIS app pools
3. Create database backup and verify
4. Launch InstallationManager
5. Select “Rotate system encryption keys” operation
6. Follow the prompts to confirm database backup
7. Monitor progress in the log window
8. Verify completion messages

9. Test system functionality before notifying users

Task 5: Configuration Inspection

Use the Configuration Viewer for troubleshooting and audit purposes.

Accessing Configuration Viewer

1. Select **View ? Configuration** from the menu
2. The viewer displays:
    - Connection strings (sanitized)
    - Key vault references
    - SMTP settings
    - Twilio settings
    - Service URLs
    - Other critical settings

Common Troubleshooting Use Cases

- **Connection Issues**: Verify database connection string
- **Email Problems**: Check SMTP configuration
- **SMS/Voice Issues**: Validate Twilio credentials
- **Key Vault Issues**: Confirm Azure Key Vault references

Security Considerations

Application Security

- **Run as Administrator**: The tool requires elevated privileges
- **Audit Logging**: All operations are logged with timestamps
- **Backup Protection**: Backups include sensitive configuration data
- **Network Access**: Tool may require access to Azure Key Vault, SQL Server, etc.

Data Protection

- **Configuration Files**: Contain sensitive connection strings and keys

- **Backup Folders**: Protect with appropriate NTFS permissions
- **Log Files**: May contain sensitive information; secure appropriately
- **Preview Mode**: Use to minimize risk before production changes

Best Practices

1. **Limit Access**: Only authorized administrators should use this tool
2. **Change Management**: Document all operations in change management system
3. **Backup Retention**: Keep backups for appropriate retention period
4. **Test First**: Use preview mode and test environments when possible
5. **Monitor Operations**: Review logs after each operation

Troubleshooting

Common Issues

Issue: "Could not find production folder"

Cause: The specified folder does not contain a valid SurePassID installation
Solution: - Verify you selected the correct folder (should contain MfaServer subfolder) - Check folder permissions - Ensure installation is complete and not corrupted

Issue: "Database connection failed"

Cause: Cannot connect to the SQL Server database
Solution: - Verify SQL Server is running - Check connection string in web.config - Confirm firewall rules allow SQL Server traffic - Validate SQL Server authentication credentials

Issue: "Key Vault access denied"

Cause: Cannot authenticate to Azure Key Vault
Solution: - Verify Azure credentials are configured - Check Key Vault access policies - Confirm network connectivity to Azure - Review Azure Active Directory permissions

Issue: "Operation failed during file copy"

Cause: File system permissions or locked files
Solution: - Ensure IIS app pools are stopped - Check NTFS permissions on target folder - Verify no files are in use by other processes - Run as Administrator

Logging and Diagnostics

Log Location

Logs are displayed in the application window in real-time. To preserve logs: 1. Click the **Copy Log** button 2. Paste into a text editor 3. Save with a meaningful filename (e.g., InstallationManager_Upgrade_2025-04-15.txt)

Log Levels

- **INFO**: Normal operational messages
- **WARNING**: Non-critical issues that should be noted
- **ERROR**: Critical failures that prevent operation completion

Diagnostic Steps

1. Review the log for ERROR messages
2. Check Windows Event Viewer for related system errors
3. Verify all prerequisites are met
4. Review the technical documentation for additional details
5. Contact SurePassID support with log file if issue persists

Support and Resources

Documentation

- **User Guide**: For step-by-step operation instructions
- **Quick Reference**: For quick command reference
- **Release Notes**: For version-specific information
- **Technical Documentation**: For architecture and development details

Support Channels

- **Website**: https://www.surepassid.com
- **Support Portal**: https://support.surepassid.com
- **Knowledge Base**: https://support.surepassid.com/general-support

Escalation Path

1. Review this guide and other documentation
2. Check the Knowledge Base for known issues
3. Contact your internal IT support team
4. Create a support ticket at the Support Portal
5. For critical issues, contact emergency support

Appendix A: Operation Reference

In-Place Upgrade

- **Risk Level**: High
- **Database Changes**: Yes
- **Downtime Required**: Yes
- **Backup Created**: Yes
- **Preview Available**: Yes
- **Typical Duration**: 15-30 minutes

New Installation Sync

- **Risk Level**: Low
- **Database Changes**: No
- **Downtime Required**: No (for new installation)
- **Backup Created**: No
- **Preview Available**: No
- **Typical Duration**: 5-10 minutes

Maintenance Release

- **Risk Level**: Low-Medium
- **Database Changes**: No
- **Downtime Required**: Yes (brief)

- **Backup Created**: Yes
- **Preview Available**: Yes
- **Typical Duration**: 10-15 minutes

Key Rotation

- **Risk Level**: High
- **Database Changes**: Yes (encrypted data)
- **Downtime Required**: Yes
- **Backup Created**: User must create
- **Preview Available**: No
- **Typical Duration**: 30-60 minutes

Appendix B: File Locations

Default Installation Paths

SurePassID Installation Root:
C:\Program Files\SurePassID Corp\SurePassID Authentication Server\

MfaServer Application:
[Root]\MfaServer\

Configuration File:
[Root]\MfaServer\web.config

Backup Location:
[Root]\Backups\[Timestamp]\

InstallationManager:
[Root]\InstallationManager\InstallationManager.exe

Azure VLE Paths

Azure VLE Installation Root:
C:\home\site\wwwroot\

Configuration:
C:\home\site\wwwroot\web.config

Appendix C: Change Management Template

Use this template for documenting changes in your change management system:

Change Request: InstallationManager Operation
Change Type: [In-Place Upgrade / Maintenance Release / Key Rotation / Config Sync]
Date/Time: [Date and Time]
Administrator: [Name]
Duration: [Estimated/Actual]
Downtime: [Yes/No]

Pre-Change State:
- Current Version: [Version]
- Database Backup: [Location and Timestamp]
- Configuration Backup: [Location]

Change Details:
- Operation Type: [Details]
- Source Folder: [Path]
- Target Folder: [Path]
- Preview Mode Used: [Yes/No]

Post-Change State:
- New Version: [Version]
- Backup Location: [Path]
- Log File Saved: [Location]

Verification Steps:
- [ ] Application starts successfully
- [ ] Users can authenticate
- [ ] Configuration settings preserved
- [ ] No errors in Event Viewer
- [ ] Services running normally

Rollback Plan:

- Database restore: [Backup Location]
- Application restore: [Backup Location]
- Estimated rollback time: [Duration]

Notes:
[Additional notes and observations]

Document Version: 1.0
Last Updated: 2025-04-15
Product Version: 2025.4.1