Agile Business Suite

Installation and Configuration Guide

Release 7.0.1047

October 2023 3826 5815-009

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product or related information described herein is only furnished pursuant and subject to the terms and conditions of a duly executed agreement to purchase or lease equipment or to license software. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information in this document or software material, including direct, special, or consequential damages.

You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Notice to U.S. Government End Users: This software and any accompanying documentation are commercial items which have been developed entirely at private expense. They are delivered and licensed as commercial computer software and commercial computer software documentation within the meaning of the applicable acquisition regulations. Use, reproduction, or disclosure by the Government is subject to the terms of Unisys' standard commercial license for the products, and where applicable, the restricted/limited rights provisions of the contract data rights clauses.

Contents

Section 1. **Introduction**

Section 2. **Agile Business Suite Overview**

Section 3. **Developer Installation**

Section 4. Developer Configuration

Section 5. Client Environment Installation

Section 6. Runtime for Windows ® Operating System Installation

Section 7. Runtime for Windows® Operating System Configuration

Appendix A. Installing Interim Corrections

Section 1
Introduction

About This Guide

This document is a guide for installing and configuring Agile Business Suite 7.0 in a standalone or network environment.

Audience

This document is primarily for those who install Agile Business Suite 7.0 either on a single workstation or on a network. It is also useful for system administrators and new users of Agile Business Suite 7.0.

Documentation Update

This document contains all the information that was available at the time of publication. Changes identified after the release of this document are included in the Information Center at https://www.support.unisys.com/absuiteic-7.0/index.jsp.

Note: *If you are not logged into the Product Support site, you are asked to do so.*

What's New in this Release

The following table lists the changes made to the document in this release:

Topic	Description
Installing Business Integrator	Added new information to the Installing Business Integrator section.

Section 2
Agile Business Suite Overview

This section provides an overview of the installation of the Agile Business Suite software.

About Agile Business Suite

Agile Business Suite is an enterprise wide application development and deployment environment for Windows® workstations. Agile Business Suite integrates into a single environment that facilities to design, develop, test, and deploy systems, in either single user or multiuser modes. The default installation provides for multiuser operation automatically. Agile Business Suite also includes the runtime system for the deployed application.

Preparing for Installation of Agile Business Suite

Agile Business Suite 7.0 prompts you with systems or software pre-requisite dialog box to confirm if all the required software has been installed before installing Agile Business Suite 7.0.

Prior to the installation of Agile Business Suite Developer or Agile Business Suite Runtime, an administrator must set up two accounts:

- Application User
- Application Administrative User

An administrator is allowed to specify which user accounts are used to represent both, the Application User and the Application Administrative User.

Refer to Creating the User Accounts or Section 3, Developer Installation.

It is recommended that for optimal security the accounts are not granted any rights or privileges over and above the minimum required privileges by Agile Business Suite to perform the necessary tasks. If you are installing Agile Business Suite Runtime on a machine which already has an installation of Agile Business Suite Developer operating, you do not need to create a second set of users.

If you wish to have the model database and runtime environment on a server, to which development workstations will connect in a multiuser system and provide debugging functionality, you should carry out these preparation and installation steps for each workstation.

Note: *It is not possible to run the setup.executable from a mapped drive using Remote Desktop. For example, you cannot access machine C, which is mapped to machine B, through Remote Desktop which is using machine A. However, you can access setup.exe from machine B so long it is not mapped and uses UNC path instead.*

The identity of an Application User is assumed by those Agile Business Suite applications that deal with the normal every day operations. The identity of an Application Administrative User is assumed by those Agile Business Suite applications that are required to perform administrative tasks, which require a higher privilege level. Thus, the likelihood of an elevation of privilege attack is minimized as the Application User, whose identity is assumed by most Agile Business Suite applications that are accessible by normal Agile Business Suite users, is a low privileged account. Those Agile Business Suite applications that are required to run under the identity of an Application Administrative User are properly secured so that normal Agile Business Suite users cannot access them, and therefore cannot launch elevation of privilege attacks.

It is not recommended that the Application Administrative User account should ever be changed after it is initially setup prior to installation. If the account needs changing for security reasons, whether the account is simply renamed or if it is completely deleted and a new account created in its place, the administrator needs to manually replace all references to the old account with the new one.

Creating the User Accounts

To create the Application User, perform the following:

1. Open Computer Management, accessible from the Administrative Tools folder in the Control Panel.
2. From the Tree view, expand System Tools\Local Users and Groups.
3. In the Users folder, right-click and select **New User** to create a user to represent the Application User. You may refer to the user by any name, however neither the name nor password should contain spaces.
4. In the **New User** dialog box:
   - Clear the **User must change password at next logon** check box.
   - Select the **Password never expires** check box.

After you have created the Application User, repeat the steps above to create a User to represent the Application Administrative User.

Note: *Once you have created the Application Administrative User, you must add that user to the Administrators group. Only the application administrator account name should be added to the administrators group. The application user account name should NOT be added to the administrators group.*

Configuring the User Accounts

It is important that these user accounts have certain User Rights. These User Rights may already exist for the users, if they have been added to a pre-existing group. If the users do not already possess the User Rights by association with an existing group, they should be configured as follows.

To configure both users, perform the following:

1. Open Local Security Policy, accessible from the Administrative Tools folder in the Control Panel.
2. In the Tree view, expand the Local Policies/User Rights Assignment.
3. Assign the following User Rights to the Application Administrative User:
    - Access this computer from the network
    - Act as part of the operating system
    - Log on as a batch job
    - Replace a process level token
4. Assign the following User Rights to just the Application User:
    - Access this computer from the network
    - Log on as a batch job
    - Log on as a service
5. Close the Local Security Policy dialog box.

Both user accounts are primarily required for the runtime functionality of the Agile Business Suite software, some of which is used for the debugging mechanism in Developer.

These user accounts are created for application purposes only. Do not log in using these account names. Log in using your own login credentials.

SQL Server Configuration

The SQL Server must be configured to allow both SQL Server and Windows authentication.

The Application User must be granted a SQL Server login to the database server that is to be used by Agile Business Suite. The login is case-sensitive and must be in the same case as specified in the Windows Security Accounts Manager database.

Configuring the Default ‘sa’ Account

When SQL Server is installed, by default the ‘sa’ account is created with a blank password. In order to ensure that unauthorized users do not gain access to your server, it is recommended that you assign a password to the ‘sa’ account. If a password is not assigned and an unauthorized user gains access using the ‘sa’ account, they have full control of all databases contained on your server.

Configuring SQL Server for Remote Access

To enable remote access to your model databases, perform the following:

1. In SQL Server Configuration Manager, enable the following protocols for the SQL Server instance hosting the model databases:
   - Named Pipes
   - TCP/IP
2. In SQL Server Management Studio, give model users permission to access your model databases – you can grant access to users individually or as Windows Groups.

Refer to the *Microsoft SQL Server documentation* for more information on configuring SQL Server.

Installing Agile Business Suite Developer

The Agile Business Suite Developer can be installed standalone on a workstation, or as a network installation with shared components. All installation types are detailed in this document.

Note: *The user performing the installation must be a Domain user, if the Application user and Application Administration user are domain accounts and the user also needs to be a member of the same domain as the Application User and Application Administration User accounts, or a member of a trusted domain.*

When you are installing Developer, it appears as the following software modules:

Module	Description
Developer	Developer consists of System Modeler, which includes a logic editor, logic validation, screen painter, debugger, and version control utilities. All development data is stored in the Model database. Developer also includes the Model Importer and Exporter which allows you to load an existing LCIF file into your model database or export the model database.
Builders	Integrates with Visual Studio.NET and enables you to generate and deploy a Runtime system for a target host directly from your Development environment.

Installing Client Environment Software

The following optional software is available for testing, viewing, and operating your Agile Business Suite system at Runtime.

You can use these products to web-enable and provide remote access to a Runtime system. When you are installing the Client Tools Environment, it appears as the following software modules.

Module	Description
Windows Forms	The Winform standalone installation comes in two versions **Winform (32-bit)** – A 32-bit application that is used to display painted forms on the screen for user interaction and can be used with Debugger. **Winform (64-bit)** – A 64-bit application that is used to display painted forms on the screen for user interaction.
Component Enabler	An environment for opening Agile Business Suite applications to current Web technology and enterprise systems running Windows operating systems. Component Enabler provides standard component interfaces to remote applications, opening them up to modern client tools and applications.
Presentation Client	Presentation Client displays GUI objects created in Developer Painter true to the way in which they were designed and to offer the functionality needed to provide an interface to remote host systems.
Business Integrator	Business Integrator provides a set of tools to assist you in developing and extending your Agile Business Suite systems to provide electronic business capability.

Module	Description
Client Framework	The Client Framework standalone installation comes in two versions **Client Framework (32-bit)** – A 32-bit version that supports client applications running on a 32-bit operating system. **Client Framework (64-bit)** – A 64-bit version that supports client applications running on a 64-bit operating system. The contents and capabilities of both versions are the same. The only difference is that each version installs the appropriate assemblies required to communicate with the runtime system from either a 32-bit or 64-bit client application. Both packages (32-bit and 64-bit) install the following components: • Windows Presentation Foundation (WPF) Client – This allows you to install the WPF Client on end-user machines that do not have AB Suite Developer. The WPF Client allows you to run Client Framework applications developed by using the WPF/XAML technology inside a WPF Container supplied and supported by Unisys. The WPF Client installation also includes the assemblies required to connect to an AB Suite runtime system. • Client Framework MVC Scaffolder Extension – This allows you to scaffold MVC Views from a set of DataModels generated by the AB Suite application. • Client Framework NuGet Packages – Direct Connect Assemblies – Use this to install and reference the Access Layer API assemblies for connecting directly to the runtime system by using COM/DCOM. – Remote Connect Assemblies – Use this to install and reference the Access Layer API assemblies for connecting to the runtime system by using the WCF Gateway. – WPF Toolkit for Client Framework – Use this to install the Toolkit assemblies for developing WPF Client applications. ***Notes:*** • *The MVC Scaffolder and the NuGet Packages require Visual Studio 2017.* • *This software must not be installed on a machine with AB Suite Developer already installed, as the AB Suite Developer installation will have the same components already installed. The Client Framework Standalone installation is intended for use on machines that do not have the AB Suite Developer available.*

You can install the Client Environment Software from the Unisys Installation Interface.

Installing Source Control

In AB Suite, you can use source control client to compare two models or a model with a set of files in a directory. Team Foundation Server (TFS) allows you to effectively manage software development projects. TFS enables multiple project objectives including source code storage, checkins and conflict resolution, and bug and issue tracking.

Refer to the TFS documentation in the *Visual Studio Online Help* for more information on minimum software and hardware configurations.

Installing Agile Business Suite Runtime

Agile Business Suite Runtime can be installed on any workstation from the AB Suite Runtime installer or as a network installation with shared components. All installation types are detailed in this document. The installation details vary depending on the host platform on which you are installing runtime.

AB Suite 7.0 Runtime is a 64-bit application and is not supported in a Native 32-bit environment. When you try to install runtime in a 32-bit environment, the error message "This installation package is not supported by this processor type. Contact you product vendor" appears.

The ExternalClassHost32 COM+ application includes the legacy 32-bit components required to host 32-bit external classes and LETSJ_SJIS conversion.

As the internal code mappings of the Japanese character set are different for the LETS-J code (on OS 2200) and the Shift JIS code (on Windows), a set of translation libraries specific to the encoding used for EAE OS 2200 is required. These libraries are the same as those used by EAE Developer. When using external classes targeting Kanji data, you must place the following libraries in the path specified by the ProductDir32 registry key, HKEY_LOCAL_MACHINE > Software > Wow6432Node > Unisys > ABSuite>(version) > SM Runtime; for example, C:\Program Files\Unisys\ABSuite7.0\bin64\X86\:

- mcutil.dll
- mcletsj.dll
- mbcsconv.dll
- eudcserv.dll

Windows Compatibility

The AB Suite 7.0 software is qualified for Windows Server 2016 Datacenter Edition and supported on the following Windows operating systems:

- Windows Server 2019 Standard, Datacenter
- Windows Server 2016 Standard
- Windows 10 Professional, Enterprise

The AB Suite 7.0 software is qualified for the following database on Windows Server 2016 Datacenter

- SQL Server 2017 Enterprise Edition

The AB Suite 7.0 software is also supported on the following databases on different Windows operating systems

For AB Suite Developer

- SQL Server 2017 Enterprise Edition is supported on:
  - Windows Server 2019 Standard, Datacenter (LTSC)
  - Windows Server 2016 Standard, Datacenter (LTSC) v1607
  - Windows 10 Professional, Enterprise (x64) October 2018 Update
- SQL Server 2017 Express, Standard are supported on:
  - Windows Server 2019 Standard, Datacenter (LTSC)
  - Windows Server 2016 Standard, Datacenter (LTSC) v1607
  - Windows 10 Professional, Enterprise (x64) October 2018 Update
- SQL Server 2012 Express (x64), Standard (x64), Business Intelligence Editions (x64), Enterprise Edition (x64) SP3 are supported on:
  - Windows Server 2016 Standard, Datacenter Update 1709
  - Windows Server 2012 R2 Standard, Datacenter w Update
  - Windows 10 Professional, Enterprise (x64) Fall Creators Update 1709

Note:

- *AB Suite is qualified using the latest security patches and updates that are available at the time of qualification. It is recommended to use the most recent security patches and updates from Microsoft.*
- *AB Suite 7.08.0 currently supports 64-bit Windows 10, Windows Server 2016 (LTSC versions), and Windows Server 2019 (LTSC versions) only. It does not support 32-bit Windows. Windows Server Semi-Annual Channel versions, such as version 1709, 1803, and 1809 are not currently supported.*
- *AB Suite 7.0 currently supports SQL Server 2017 only. Please contact AB Suite Support if you require support for an older level of SQL Server.*
- *Microsoft OLE DB Driver 18 for SQL Server is required for AB Suite 7.0 Administration Tool, as previous OLEDB drivers do not support TLS 1.2. Please download 64- bit drivers and install them from. TLS 1.2 or later is required, earlier TLS and SSL levels are not supported.*

For AB Suite Runtime

- SQL Server 2017 Enterprise Edition is supported on:
  - Windows Server 2019 Standard, Datacenter (LTSC)
  - Windows Server 2016 Standard, Datacenter (LTSC) v1607

SQL Server 2017 Express, Standard Edition is supported on:

- Windows Server 2019 Standard, Datacenter (LTSC)
- Windows Server 2016 Standard, Datacenter (LTSC) v1607

Note:

- *Windows 10 can be used for testing purposes only and is not supported in the AB Suite Windows Runtime production environments. Latest updates are required for testing.*
- *Windows Operating System editions, such as Windows Home or Server Core Editions are not supported and might not work with AB Suite 7.0 Runtime for Windows.*
- *SQL Server Express and Developer Editions can be used for testing purposes only and is not supported in AB Suite Windows Runtime production environments. However, latest updates are required for testing.*
- *AB Suite 7.0 currently supports 64-bit Windows 10, Windows Server 2016 (LTSC versions), and Windows Server 2019 (LTSC versions) only. It does not support 32-bit Windows. Windows Server Semi-Annual Channel versions, such as version 1709, 1803, and 1809 are not currently supported.*
- *AB Suite 7.0 Runtime for Windows currently supports SQL Server 2017 only. SQL Server Developer Edition is not supported for production usage.*

Installation Problem Reporting

Because Agile Business Suite relies on the underlying operating system and network software, details of the environment are vital to the resolution of problems. When reporting problems, ensure the following information is supplied:

- The operating system and version number used on the workstations, for example, Windows Server 2016 Datacenter installed.
- All networking software and versions, the network server software and level, and the workstation client software and version.
- Error and log files.

Prerequisites for Installing in VDI Environment

In Windows Server 2016 Datacenter Virtual Desktop Infrastructure (VDI) that does not have internet connectivity, you might encounter installation issues while installing AB Suite Developer, Client Tools Component enabler, Runtime, Presentation Client, and Business Integrator. The installation issues might be related to the missing certificates, which need to be imported into the VDI environment. You must export the following certificates from a machine that has internet connectivity and then import them into a machine where AB Suite is installed in a VDI environment without internet connectivity:

- VeriSign Class 3 Public Primary Certification Authority - G5
- GlobalSign Root CA

Note: *You can also use the signtool utility against the AB Suite installed CAB files to verify the missing files.*

Installing Agile Business Suite in a Distributed Runtime Configuration

Agile Business Suite can be installed on a network as a distributed system, with a Runtime Server, a Database Server and one to many Developer workstations. Developer can also be installed on the Runtime Server or the Database Server as required.

To install Agile Business Suite in a distributed runtime configuration, refer to the following sections:

- Configuring Users and Network Communications
- Installing Visual Studio
- Installing Agile Business Suite Runtime
- Installing Agile Business Suite DB Migrate Utilities
- Installing Agile Business Suite Developer
- Installing SQL Server 2017

When you run the executable file, it reads the configuration file specified in the Target box to set up the connection parameters required to connect to the runtime system.

Once the distributed system is installed, to deploy an application to a distributed configuration:

1. Create, import, or open a model in Agile Business Suite Developer.
2. Configure the Business Segment to be deployed for remote deployment.
3. In the Installation section of the Segment's deployment properties, set the deployment host to the remote host.
4. Configure the Business Segment to use the remote Database Server registration.

   In the Persistence section of the Segment's deployment properties, set the Database Server Registration to the mapping created on the remote runtime server.

Configuring Users and Network Communications

Before installing Agile Business Suite and supporting software, you need to create user accounts and configures them in the active directory of the domain controller, by performing the following

1. In the user properties for your domain Application Administrative User, on the Delegation tab, select **Trust this user for delegation to any service (Kerberos only)** option (this option might differ depending on your operating system).

   Note: *In Windows Server 2010 and later version domains, to provide delegation privileges to the Application Administrator User account and mark it as "Account trusted for delegation", you should assign Service Principal Name (SPN) to the Application Administrator User account in the active directory.*

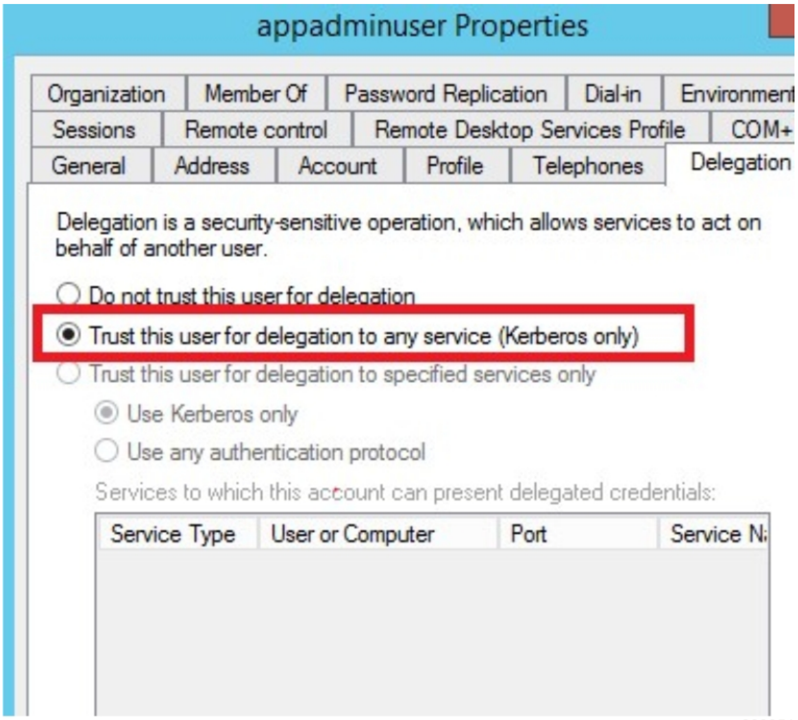
   For example, to assign an SPN name 'https/AppAdminUser' to AppAdminUser account, run the following setspn command on domain controller:

   ```
   setspn –a https/AppAdminUser AppAdminUser
   ```

   where, the first parameter, https/AppAdminuser, is an SPN name and the second parameter, AppAdminUser, is an account name.

   You can also prefix a domain name with the account name, for example,

   ```
   setspn –a https/AppAdminUser MyDomain\AppAdminUser
   ```



appadminuser Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

● Trust this user for delegation to any service (Kerberos only)

○ Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N

009051

2. If you are using Web Services, install IIS on the Runtime Server.

   Agile Business Suite 7.0 supports Web services on the Windows runtime in an IIS 10.0 environment.

   The IIS 10.0 Web Server is available on the following platform:

- Windows Server 2016

  Note that the IIS 6 Management Compatibility component needs to be installed for Web Services to work on IIS 10.0. The IIS 6 Management Component includes:

- IIS Metabase and IIS 6 configuration compatibility

3. If you are using MSMQ protocol adapters, install Message Queueing on the Runtime Server.
4. On the Database Server, you need to enable the Application user to remotely launch and activate COM+ applications.
5. Add the Application Administrative User to the Administrators group on the Runtime and Developer Severs. Refer to Preparing for Installation of Agile Business Suite for more information.
6. Configure the local security policy for the Application User and the Application Administrative User as described in Preparing for Installation of Agile Business Suite
7. Add the Application User and Application Administrative User to the Distributed COM Users local group and the Network Access local group on the Runtime and Developer Servers.
8. Enable Distributed COM on the Application Server and the Development Server by performing the following:

   a. Point to the bottom-left corner of the screen to enable the Start icon, right-click **Start**, and then click **Run**.

   b. Type dcomcnfg in the Run dialog box and then press **Enter**.

      The Component Services window appears.

   c. In the left pane, expand **Component Services** and then expand **Computers**.

   d. Right-click **My Computer** and select **Properties** from the context menu.

      The **My Computer Properties** dialog box appears

   e. On the **Default Properties** tab, select **Enable Distributed COM on this computer**.

   f. Click **OK**.

Installing Visual Studio

Install Visual Studio 2017 Professional version 15.9.7 or higher on each developer machine. Windows Server 2016 also installs the matching .NET Framework version 4.7.2.

Note: *You must use the recent security patches and updates from Microsoft.*

Installing Agile Business Suite Runtime

Install the full Agile Business Suite Runtime on the Runtime Server with the following custom options:

- Runtime
- AdminTool

Installing Agile Business Suite DB Migrate Utilities

The installation of AB Suite DB Migrate Utilities allows AB Suite DB Migrate Utilities for SQL Server 2017 to be installed on a standalone SQL Server Database Server. This installation allows DB migrate utilities to import runtime data from EAE. Install Agile Business Suite DB Migrate Utilities component on the Database Server with the following custom options:

- AdminTool
- DB Migrate Utilities

You can view these options when you install Runtime on your workstation.

Installing Agile Business Suite Developer

Install Agile Business Suite Developer on each Developer workstation.

Installing SQL Server 2017

Install SQL Server 2017 Enterprise Edition on the Database Server and any Developer workstation. Ensure that the following components are also installed.

For database migration install:

- Integration Services
- Analysis Services
- Legacy Components

For the enterprise management tools install:

- Connectivity components
- Management Tools (SQL Server Management Studio is installed separately)

Installation of SQL Server 2017 does not add the BUILTIN\Administrators group as a sysadmin by default. This affects the creation of runtime databases via the Runtime Administration Tool.

You can perform either one of the following to overcome this situation:

- Specify the BUILTIN\Administrators group in the Database Engine Configuration dialog box during the installation of the SQL Server 2017.
- Add the Application Administrative User account as sysadmin in SQL Server 2017. You need to do this for every Instance of SQL Server 2017.

Distributing Configuration Files

You can connect the Direct Connect client applications, such as Winforms and Client Framework to the AB Suite runtime system running on a different machine in the same domain.

To connect the Direct Connect client applications to the AB Suite system running on a remote machine, perform the following:

1. Share the folder where you have stored the configuration file on the network.
2. Modify the following tags in the configuration file:
   - <RuntimeServer> – Set this tag to the machine name where the runtime system is deployed. This can also be the IP address of the server.

     For example, <RuntimeServer>ustr-erl2-9999</RuntimeServer>
   - <DownloadServerUrl> – Set this tag to the location where the DLLs that implement the client forms are located.

     For example,

     If you want to connect the Winforms to the AB Suite runtime system on a different machine, you must modify the <DownloadServerUrl> tag in the Winform config file (for example, Ispec.xml) as follows:

     <DownloadServerURI>\\<IP Address of Remote Runtime System>\<SharedFolderName>\<configuration name>\<segment name>\Interfaces\Winforms\ Core\Bin </DownloadServerURI>

     If you want to connect the WPF Client to the AB Suite Client Framework runtime system on a different machine, you must modify the <DownloadServerUrl> tag in the WPF Client config file (for example, <TechnologyFolderName>_Config.rtxml) as follows:

     <DownloadServerURI>\\<IP Address of Remote Runtime System>\<Visual Studio Projects Folder>\<Solution name>\Access Layer API Deploy</DownloadServerURI>

   Notes:

   - *A default Winform config file, Ispec.xml, is generated when you build the AB Suite application in the following location:*

     <package installation directory>\<configuration name>\<segment name>\Core\Bin\Ispec.xml
   - *A default WPF Client configuration file, <TechnologyFolderName>_Config.rtxml, is generated when you build the AB Suite Client Framework application in the following location:*

     <Visual Studio Projects Folder>\<solution name>\Access Layer API Deploy\<TechnologyFolderName>_Config.rtxml

   You can copy the configuration files to a different location on the system and customize it as per your requirement.
3. Ensure that the standalone Client Framework or Winform Client is installed on the client machine.

4. Create a shortcut of the executable file on the desktop of the client machine.

   Note: *When a 32-bit standalone Client Framework or Winform Client is installed, the executable file is located in the following path:*

   C:\Program Files (x86)\Unisys\AB Suite 7.0\Bin

   When a 64-bit standalone Client Framework or Winform Client is installed, the executable file is located in the following path:

   C:\Program Files\Unisys\AB Suite 7.0\Bin

5. Right-click the shortcut, and select **Properties**.

   The **Properties** dialog box appears.

6. In the **Target** box, enter the IP address of the client machine and the location of the configuration file.

   For example, <IP Address of Client Machine>\
   C:\Users\appadminuser\Documents\Visual Studio 2017\Projects\<app name>\Access Layer API Deploy\WPF_Config.rtxml

7. Click **OK**.

When you run the executable file, it reads the configuration file specified in the Target box to set up the connection parameters required to connect to the runtime system.

Configuring for Distributed Deployment

To finalize the configuration for distributed deployment, perform the following:

1. On the Runtime Server, create a remote database server registration that points to the default instance of SQL Server on the Database Server machine.
2. Once you have created a database server registration, you can add new runtime databases or attach pre-existing databases. The Admin Tool detects any existing AB Suite databases, including the databases in the earlier releases and automatically re-attaches the databases to be used with AB Suite 7.0.

Section 3
Developer Installation

This section describes how to install Agile Business Suite Developer.

Required Software Configuration

The system software configuration required to support Agile Business Suite Development client workstations are detailed in the following table.

Required Software	Comments
• Windows Server 2016 Datacenter (LTSC) v1607	Windows 10 Professional, Enterprise (x64) October 2018 Update, or Windows Server 2019 (LTSC) Standard, Datacenter, or Windows Server 2016 (LTSC) Standard v1607 supports AB Suite development environment. AB Suite 7.0 currently supports 64-bit Windows 10, Windows Server 2016 (LTSC versions), and Windows Server 2019 (LTSC versions) only. It does not support 32-bit Windows. Windows Server Semi-Annual Channel versions, such as version 1709, 1803, and 1809 are not currently supported. Agile Business Suite 7.0 Developer runs in a 64-bit WOW64 environment.

Required Software	Comments
• Visual Studio 2017 Professional version 15.9.7 or later and • Team Foundation Server (TFS) 2018 Update 3 or later	Team Foundation Server 2018 requires SQL Server 2017. Read the operating system and SQL Server pairing requirements for the supported Team Foundation Server levels at the following website: https://www.visualstudio.com/en-us/docs/setup-admin/requirements On 64-bit operating systems, Visual Studio 2017 runs in WOW64 environment. Visual Studio Community Edition, Express Edition, and Test Professional Editions are not supported. ***Notes:*** • *Visual Studio 2017 version can change frequently. Refer to the AB Suite 7.0 Software Qualification and Support Matrix for the updated Visual Studio 2017 version details.* • *When you install Visual Studio 2017, you have to select the required workloads and components necessary to support the installation of AB Suite 7.0. See Installation of Visual Studio 2017 for information on the components that you have to select when you install Visual Studio 2017.* • *AB Suite 7.0 currently supports Visual Studio 2017 and TFS 2018. Please contact AB Suite Support if you require support for an older level of TFS.*
One of the following: • SQL Server 2017 Enterprise Edition • SQL Server 2017 Express, Standard	The installation proceeds successfully if SQL Server is not installed. However, before you start using Developer, you must either install a database server or have access to another machine with a database server installed. ***Notes:*** • *SQL Server 2017 Native Client is required for Developer installation that do not already have SQL Server installed locally.* • *AB Suite 7.0 currently supports SQL Server 2017. Please contact AB Suite Support if you require support for an older level of SQL Server.* • *If you are using SQL database, ensure that it is configured as described in SQL Server Configuration.* • *SQL Server 2017 need not be installed on a Developer workstation when the Model database is on another machine. However, it is required only when you need a local Model database. If the model database is on another machine, then SQL Server Native Client is a requirement for the Developer workstation.*
Microsoft SQL Server Management Studio	SSMS 17.x is required.

Required Software	Comments
Microsoft Visual C++ Redistributable for Visual Studio 2017 latest update	No comments for this requirement.
Microsoft Visual Studio 2015 Shell (Isolated)	This is a mandatory pre-requisite for AB Suite Developer installations. This will be installed automatically when installing SSMS 17.x.
Microsoft OLE DB Driver for SQL Server	This is an optional software. ***Note:*** *Microsoft OLE DB Driver for SQL Server need not be installed for MCP Runtime applications that use HDBA with Debugger sessions, because MCP Debugger sessions using HDBA uses Unisys OLE DB driver.*
Microsoft SQL Server 2017 Native Client	This is a mandatory pre-requisite for AB Suite Developer installations that do not already have SQL Server installed.
.NET Framework 4.7.2	.NET Framework 4.7.2 or later is required. ***Note:*** *.NET 4.7.2 is supported and required on Windows Server 2016.*
Java Software Development Kit v1.6 or later	This is used for generating Java based applications. ***Notes:*** • *Java Software Development Kit v1.8 is supported. This excludes custom generators.*
Enterprise Output Manager 13.0 (64-bit)	This is an optional supported application. ***Note:*** *On 64-bit operating systems, EOM runs in WOW64 environment as it is a 32-bit application.*

Required Agile Business Suite Software

Due to the inter-relationships between the components of the Agile Business Suite software, the Agile Business Suite Runtime for Windows Release 7.0 software for the target host platform is required, if you wish to generate and deploy an Agile Business Suite system.

Installation of Visual Studio 2017

When you install Visual Studio 2017, you have to customize the installation by selecting the required features to support the installation of AB Suite 7.0.

To select the required features, perform the following:

1. Select the **Workloads** option.

   a. Under **Windows**, select the following:

      - .NET desktop development
      - Desktop development with C++

   b. Under **Web & Cloud**, select the following:

      - ASP.NET and web development

   c. Under **Other Toolsets**, clear the **Visual Studio extension development** check box.

      Note: *If this option is selected, an error message appears when you install Developer and therefore you will not be able to proceed with the installation.*

2. Select the **Individual Components** option.

   The required components to support the installation of AB Suite 7.0 are selected automatically based on the features you select in the Workloads option. However, you have to select the following components manually:

   a. Under **.NET**, select the following components:

      - .NET Framework 4.7.2 SDK
      - .NET Framework 4.7.2 targeting pack

   b. Under **Code tools**, select the following components:

      - Help Viewer

        Note: *If you do not select Help Viewer, you cannot view the Developer online help in Help Viewer.*

Minimum Hardware Requirements

Developer is installed on stand-alone workstations. Minimum requirements for this configuration are described below.

Workstations

Developer is an I/O intensive application because all objects are stored in the model and updated constantly as each object changes.

Windows is also I/O intensive when all applications cannot reside in memory. This means that disk transfer rates are a critical factor in workstation performance. Faster disk drives and increased RAM provides performance benefits.

The following table shows the minimum recommended hardware requirements for a workstation when Developer is installed, either on its own, or together with Builder or Version Control.

Hardware	Developer Workstation	Build Server	Runtime Server	Model Server
Processor	2 core, 2 GHz (x86)	2 core, 2 GHz (x86)	4 core, 2 GHz	2 core, 2 GHz (x86)
RAM	4 GB	4 GB	8 GB	4 GB
Disk space*	200 GB	200 GB	200 GB	200 GB
Operating System	32-bit Client Operating System	32-bit Client Operating System	64-bit Server Operating System	32-bit Client Operating System
Other	SVGA or LCD monitor			

The following table shows the recommended hardware for a workstation:

Hardware	Developer Workstation	Build Server	Runtime Server	Model Server
Processor	Quad Core Intel Core i7 (equivalent or better)	Dual Core Intel Core i7 (equivalent or better)	Quad core configuration Intel i7/ Xeon (3 GHz) (equivalent or better)	Dual core Intel Core i7 (equivalent or better)
RAM	16 GB or higher	8 GB or higher	16 GB or higher	8 GB or higher
Disk space*	500 GB	500 GB	500 GB Operating System Drive	500 GB
Operating System	64-bit Operating system	64-bit Server Operating System	64-bit Server Operating System	64-bit Server Operating System
Other	Large, wide-screen LCD monitor	LCD	Active Directory domain membership	

* Additional disk space is required if the Microsoft SQL Server database is stored on this machine. The required space varies depending on the size and complexity of the system.

For the Model Database

The disk space required for the model database depends on the size of the Specification being developed. This includes the number of <<Ispec>> classes, Reports, lines of logic, and Global Logics.

Due to the extensive re-engineering that has been carried out in this version of Developer, and the efficiency of the Microsoft SQL Server database, the disk space required for a Model database is significantly less than was required for previous releases of Enterprise Application Developer.

Preparing Your Network for Developer

Network traffic can be a significant factor in the overall performance of Developer with a multiuser SQL database.

Before installing Developer, you should tune your network to minimize traffic congestion. This ensures that your network handles the interaction between Developer and the database to provide optimum performance.

Access Rights to Drives, Directories, and Files

You must give the Application User and the Application Administrative User full read and write access rights to the drive and directory in which the Microsoft SQL Server database of a user is located.

The Application User and the Application Administrative User must have read and write access rights to their nominated working directories.

Access to Font Files

The Application User and the Application Administrative User must have read and execute access to the fonts that Developer uses. This is necessary in order to correctly display the fonts used in the Painter and the Logic Editor, and for creating Help screens. Developer uses these fonts: LINCDEFAULTNEW, and LINCDEFAULTNEWBOLD. These fonts are stored in the directory **C:\Windows\Fonts**.

Installing Developer on a Workstation

Developer can be installed on any workstation from the Unisys Installation Interface. It can also be installed to operate remotely by using the Microsoft Remote Desktop Services.

Prerequisites

Setting Access Rights

If the Developer installation process attempts to overwrite a system file and detects that you do not have Administrator access rights, an error message appears and the installation process exits.

Windows operating system access rights are set by the Computer Management program. This can be accessed by clicking the Administrative Tools (Common). If you are unable to set Windows operating system access rights, contact the System Administrator for your site. Note that if Active Directory is in use, you might need to set these permissions through a group policy.

Note: *If the Developer installation process finds system files that requires to be updated, you are prompted to reboot your machine before running Developer.*

On Windows 10 and later operating systems, you do not need to run Developer as an Administrator while using setup.exe for installation.

Refer to Preparing for Installation of Agile Business Suite for more information on how these user accounts can be created manually.

Disable Spyware Applications

If you are using any spyware application, such as Spy Sweeper or Ad-Aware, you have to disable it before executing the installation or uninstallation process.

Failure to do so might result in the following error:

1935 – An error occurred during the installation of assembly.

Performing the Developer Installation

After an administrator has created the required users and configured them correctly, you can begin the installation of Developer.

You can also create the required users when you are installing developer.

To install Developer, perform the following:

1. Double-click CDBrowser.exe.

   The Unisys Installation Interface appears. This interface controls the installation process.

2. Click **Development Environment**.

   The InstallShield Wizard appears.

   Note: *When this wizard appears, the installation program performs the prerequisite checks. If any of the prerequisite checks fail, then a message appears and the installation is terminated. If the checks are successful, you can continue with the installation.*

3. On the InstallShield Wizard, click **Next**.

4. Select **I accept the terms in the license agreement** option, after you read and accept the terms in the license agreement, and then click **Next**.

5. Select the target drive and directory for the installation, if you do not want to accept the default installation location, and then click **Next**.

Note: *You cannot install different versions of AB Suite Developer, such as 5.0, 6.1, or 7.0 on the same machine.*

6. Select either of the following setup type:

   - **Complete**

     Select this option to install the essential components of Developer and Target Builders. The Developer components consist of System Modeler, Debugger, Version Control Tools, Documentation, Builder, Automated Test Tool, Client Framework components, and Target Builders for Windows and MCP.

     Notes:

     - *Documentation*

       If Microsoft Help Viewer is installed, Documentation feature is installed when System Modeler is installed on a workstation. When documentation is installed on your workstation you can view the AB Suite online help in help viewer.

     - *Automated Test Tool*

       The ATT package is installed when System Modeler is installed on a workstation. ATT supports recording of test cases for AB Suite applications and AB Suite Client Framework applications. If you want to record test cases with Component Enabler Client you need to install Component Enabler.

     - *Client Framework*

       Although all Client Framework components are installed when System Modeler is installed on a workstation, you might need to install additional development tools, such as Microsoft Blend, in your environment depending on the technologies you choose for developing your client applications.

   - **Custom**

     Select this option to customize the components that you want to install and click **Next**.

     The following options appear:

     - System Modeler
     - Builders
     - Documentation

     System Modeler

     This is a mandatory feature. It installs the Developer software, which includes all the functionally required in Developer.

     Builders

     Select this option to install the Builder software, which allows you to build and deploy an application in both Windows and MCP runtime environment.

     The Builder software should be installed if you want to run the Debugger.

     Documentation

Select the Documentation feature to install the AB Suite Documentation. When you install Documentation you can view the AB Suite Developer online help through the help viewer. However, Microsoft Help Viewer must be installed.

Note: *You can also view the AB Suite online help through the browser even if you do not install the Documentation feature.*

7. Click **Next** and select any of the following options to create a new Application User or to select an existing Application User:

   - Select an Application User from existing user accounts
   - Create a new Application User account.
   - Allow Installation to automatically create the Application User.

   ### Select an Application User from existing user accounts

   You can select this option when you have an Application User created prior to the installation.

   To select an Application User from existing user account, perform the following:

   a. After you select, **Select an Application User from existing user accounts** option, click **Next**.

   b. Enter the following credentials for the Application User:

      - Domain Name — Enter the Domain name of which this user is a member. If the Application User is a local user, you can simply accept the period character for the domain name or enter the name of the local machine. However, if the user has been created as a member of a network domain, the name of that domain should be entered here. This could occur if the database that Developer connects to is on a machine other than the local machine.
      - User Name — You can either type the Application User Name or click Browse and select the Application User name from the Select a User Name dialog box.
      - Password — Enter the password for the user name on the chosen domain.

   ### Create a New Application User Account

   You can choose this option to create a new Application User.

   To create an Application User, perform the following:

   a. After you select, **Create a New Application User Account** option, click **Next**.

   b. Enter the following credentials for the new Application User:

      - Domain — Displays the domain name of the computer. You can either retain the domain name or type “.”.
      - User Name — Enter the new Application User name.
      - Password — Enter a password for the new Application User.
      - Confirm Password — Re-enter the password.

   c. Click **Create**.

A message box appears confirming the creation of the application user.

d. Click **OK** on the message box.

Note: *The local security policy user is automatically set by the installation. Refer to Configuring the User Accounts for more information.*

Allow Installation to Automatically Create the Application User

You can choose this option to allow the installation to create a default Application User.

To automatically create an Application User, perform the following:

a. After you select, **Allow Installation to Automatically Create the Application User** option, click **Next**.

b. Enter the following credentials for the new Application User:

- Display Name — Displays the domain name of your system.
- User Name — Displays ABSuite70AppUser, which is the default user name created for AB Suite application user.

  Note: *You cannot edit the domain name and user name.*
- Password — Enter a password for the new Application User.
- Confirm Password — Re-enter the password.

c. Click **Create**.

A message box appears confirming the creation of the application user.

Note: *The new Application User is created by using this option only when it is used for the first time. If the user already exists in the system and you use this option, you will be prompted with a message –"The default user already exists. Please enter the password."*

d. Click **OK** on the message box.

Note: *The local security policy for the user is automatically set by the installation. Refer to Configuring the User Accounts for more information.*

8. Click **Next** and select any of the following options to create a new Application Administrative User or to select an existing Application Administrative User:

- Select an Application Administrative User from existing user accounts
- Create a new Application Administrative User account.
- Allow Installation to automatically create the Application Administrative User.

Select an Application Administrative User from Existing User Accounts

You can select this option when you have an Application Administrative User created prior to the installation.

To select an Application Administrative User from existing user account, perform the following:

a. After you select, **Select an Application Administrative User from existing user accounts** option, click **Next**.

b. Enter the following credentials for the Application Administrative User:

- Domain Name — Enter the Domain name of which this user is a member. If the Application Administrative User is a local user, you can simply accept the period character for the domain name or enter the name of the local machine. However, if the user has been created as a member of a network domain, the name of that domain should be entered here. This could occur if the database that Developer connects to is on a machine other than the local machine.
- User Name — You can either type the Application Administrative User Name or click **Browse** and select the Application Administrative User name from the Select a User Name dialog box.
- Password — Enter the password for the user name on the chosen domain.

Create a New Application Administrative User Account

You can select this option to create a new Application Administrative User.

To create an Application Administrative User, perform the following:

a. After you select, **Create a New Application Administrative User Account** option, click **Next**.

b. Enter the following credentials for the new Application Administrative User:

   - Domain — Displays the domain name of your system. You can either retain the domain name or type ".".
   - User Name — Enter the new Application Administrative User name.
   - Password — Enter a password for the new Application Administrative User.
   - Confirm Password — Re-enter the password.

c. Click **Create**.

   A message box appears confirming the creation of the application administrative user.

d. Click **OK** on the message box.

Note: *The local security policy user is automatically set by the installation. Refer to Configuring the User Accounts for more information.*

Allow Installation to Automatically Create the Application Administrative User

You can choose this option to allow the installation to create a default Application Administrative User.

To automatically create an Application Administrative User, perform the following:

a. After you select, **Allow Installation to Automatically Create the Application Administrative User** option, click **Next**.

b. Enter the following credentials for the new Application Administrative User:

   - Display Name — Displays the domain name of your system.
   - User Name — Displays ABSuite70AppAdmin, which is the default user name created for AB Suite application user.

     Note: *You cannot edit the domain name and user name.*

- Password — Enter a password for the new Application Administrative User.
- Confirm Password — Re-enter the password.

c. Click **Create**.

A message box appears confirming the creation of the application administrative user.

d. Click **OK** on the message box.

Note: *The new Application Administrative User is created by using this option only when it is used for the first time. If the user already exists in the system and you use this option, you will be prompted with a message –"The default user already exists. Please enter the password."*

9. Click **Next**.

10. In the Data folder screen that appears, you can either install the data files to the default location, C:\AB Suite 7.0\Data\, or click **Change** to install the data files to a different location.

    This is the location of the Runtime Data directory that stores various data files, such as log files and configuration files.

11. Click **Next**.

12. In the Builder Cache Folder that appears, select the path for the Builder Cache.

    The compressed copies of files generated by Builder are stored in this location. This location can be changed after the installation is complete from the Tools, Options dialog box.

    When systems are generated to any target platform and multiple workstations are used for this purpose, all workstations must use a shared directory. This ensures that all the shared workstations create, modify, and read the same files in the BuilderCache directory.

    To do this, perform the following:

    a. Browse to the location of the BuilderCache directory.

    b. Right-click the BuilderCache directory, and select **Properties**. The **BuilderCache Properties** dialog box appears.

    c. Select the **Sharing** tab and choose **Share this folder** option.

    d. Click **Permissions** and add the remote user.

    e. In the Permissions for the BuilderCache, select the **FullControl** check box for the remote user.

    f. On the remote machine, add the shared BuilderCache directory as a mapped network drive.

    g. Set the network drive as the path for the BuilderCache directory during the Agile Business Suite installation on the remote machine.

    In a multi user environment, it is recommended that all users select a shared location for the Builder Cache. This prevents unnecessary re-generates of already generated and unchanged files.

Setting the Builder Cache and Builder Output Path

You can set the builder cache path and the builder output path as follows:

Builder Cache Path

When you install AB Suite Developer, you can either set the builder cache path for All Users or for Current User only.

If you want to set the builder cache path for all users, clear the **Set the Builder Cache Path for this user** only check box. This check box is not selected by default.

If you want to set the builder cache path for the current user, select the **Set the Builder Cache Path for this user** only check box.

If there are any installation restrictions on using the C drive, you can change the builder cache path at this stage, during the installation, by clicking the **Change** button in the InstallShield Wizard.

Builder Output Path

The builder output path, however, can be changed from Visual Studio only. This change affects the Current User and not All Users.

To change the builder output path, perform the following steps:

a. Start Visual Studio after the installation of AB Suite is complete.

b. From the **Tools** menu, select **Options**.

   The **Options** dialog box appears.

c. In the left pane, expand **System Modeler**, expand **Builder**, and then select **General**.

d. In the right pane, enter or browse to the location of your choice in the **Location of Build Output** box.

   Note: *You can also enter or browse to a location of your choice in the* ***Location of Cache for generated files*** *box.*

   If there are any restrictions on using the C drive, you can change the builder output path to an alternative drive of your choice.

13. Click **Next**.

14. In the Ready to Install the Program screen, click **Install** to begin the Installation.

    If you want to change any of the installation settings you can click **Back** and change the settings. The Installing Agile Business Suite 7.0 Developer screen displays the progress bar.

    At the completion of the installation, the Installation Complete Screen appears.

    This screen displays the following options:

    - **Show the readme file** — displays the readme file when you select the check box and click Finish. You can clear the check box if you do not want to view the readme file. This check box is not selected by default.
    - **Show the Windows Installer log** — display the AB Suite <version>

Runtime.log file when you select the check box and click Finish. You can clear the check box if you do not want to view the log file. This check box is not selected by default.

15. Click **Finish** to complete the installation.

Silent Installation

The Developer Installation Package is in the .msi format and supports Silent Installation through the use of the msiexec.exe utility. When the command line argument "/qn" is passed to the utility, the installation of the Developer Installation Package proceeds without Graphical User Interface (GUI) that is, there are no dialog boxes or user prompts requesting for information, such as the installation directory. The progress of the installation, indicating success or failure, is written to a log file. The log file includes the status, warnings, and error messages.

Performing Silent Installation of Developer

To install the Developer Installation Package in silent mode, execute the following command from the command prompt:

```
“:> msiexec.exe /i “<path of the AB Suite 7.0 Developer.msi>\AB Suite7.0 Developer.msi” /qn <parameters>"
```

The commands or parameters to execute the AB Suite package are as follows:

Commands or Parameters	Values
msiexec /i	Example: <default>\AB Suite 7.0 Developer\Product Configuration 1\Release 1\DiskImages\Disk1\AB Suite 7.0 Developer.msi
/qn INSTALLDIR =	Example: C:\Program Files\Unisys\AB Suite 7.0\
AgreeToLicense	Yes
ADDLOCAL	ALL
APP_USER_DOMAIN=	.
APP_USER_NAME=	Example: AppUser
APP_USER_PASSWORD=	Example: App1User
APP_ADMIN_DOMAIN=	.
APP_ADMIN_NAME=	Example: AppAdminUser
APP_ADMIN_PASSWORD=	Example: App1AdminUser
PASSDATA=	Example: C:\AB Suite 7.0\Data\
/l*v	Example: C:\Temp\AB Suite 7.0.Log

Where,

msiexec is the executable program of the Windows Installer to interpret installation package and install products on the target location.

/i switch is used to install the package from the command line.

/qn switch is used to suppress the dialog boxes displayed for input and output to the user.

INSTALLDIR is a property for specifying the location where the Windows Installation Package is installed.

/l*v switch is used to create a log file.

Following is an example to install Developer through Silent Installation from the command prompt:

```
msiexec.exe/i
/qn/ norestart INSTALLDIR="C:\Program Files\Unisys\AB Suite 7.0\" AgreeToLicense=Yes ADDLOCAL=
ALL APP_USER_DOMAIN=APP_USER_NAME=AppUser APP_USER_PASSWORD=App1User
APP_ADMIN_DOMAIN=APP_ADMIN_NAME=AppAdminUser APP_ADMIN_PASSWORD=App1AdminUser
PASSDATA="C:\AB Suite 7.0\Data\"
/l*v "C:\TEMP\AB Suite 7.0 Developer.log"
```

Installing Developer with Windows Remote Desktop Services

It contains instructions on how to install and configure Developer with Microsoft Windows Server 2016 and above Remote Desktop Services.

Note: *Remote Desktop Services installation is recommended when you want to use a shared model database and have all the development environments on the same physical machine.*

What are Remote Desktop Services?

Remote Desktop Services allows a single server to be used for multiple users, with each user having a separate virtual environment on the Remote Desktop Services server. All processing is performed by the Remote Desktop Services server.

Users access the server using a client containing only the minimum software necessary to boot the device, establish a connection to the server, and present the user interface. This type of client is sometimes called a Thin Client.

Windows Server 2016 provide integrated support for a Thin Client environment in the form of Windows Server 2016 Remote Desktop Services.

Recommended Configuration

Configure a Remote Desktop Services server installation on a Windows network so that all users who log in to the network and use a Remote Desktop Services client session are able to use required Developer components.

In this recommended configuration:

- Users log in to the Local Area Network (LAN) using a Windows Remote Desktop Services client session and start Developer. Dial-in connections, as well as direct connections, might be used.
- Developer clients connect to the Developer application on the network.

Requirements for a Remote Desktop Services Installation

Before installing and configuring Remote Desktop Services, ensure you have the following:

- A network directory (usually a location on the file server), from which a Developer client installation can be performed.
- A machine with Microsoft Windows Server, connected to the network, on which the Version Control Server (if required) and Model database are to be installed. This is referred to as the Server machine.
- A machine with Microsoft Windows Remote Desktop Services installed and connected to the network. This is referred to as the Remote Desktop Services server.
- A *Root Drive* for each user on the network, which is mapped to the user's home directory on the network. For example, each user has drive letter H: as the root drive mapped to a directory on the Developer Server machine. It is represented by the %ROOTDRIVE% environment variable on the Remote Desktop Services server.

Installation Procedure

For the purposes of this example installation, it is assumed that:

- Each user's *Root Drive* (%ROOTDRIVE% variable) is mapped to drive letter H:.
- The %SYSTEMROOT% environment variable on the Remote Desktop Services server is set to C:\Wtsrv.
- Required user accounts have been created on the Remote Desktop Services server.

Setting Access Rights

In order to install Developer on a Windows Remote Desktop Services server, you need to have **Administrator** access rights to the Remote Desktop Services server. This is required because some Windows system files might be overwritten during installation, and only users with Administration access rights have permission to overwrite system files.

If the Developer installation process attempts to overwrite a system file and detects that you do not have Administrator access rights, an error message is displayed and the installation process exits.

Windows operating system access rights are set by Computer Management MMC snap-in. You can access this by pointing to and clicking the **Start** icon in the bottom-left corner of the screen, right-clicking a blank part of the **Start** screen, selecting **All apps**, and then clicking **Administration Tool** under **Agile Business Suite 7.0**. Alternatively, after clicking the **Start** icon, type **Administration Tool** on the desktop to locate and select the application from the **Start** screen. If you are unable to set Windows operating system access rights, see the System Administrator for your site.

Note: *If the Developer installation process finds system files that need updating, you will be prompted to reboot your machine before running Developer.*

Installing Remote Desktop Services

1. When installing Windows Server 2016 on your Remote Desktop Services server machine, you must install the following components:

   - **Remote Desktop Services**
   - **Remote Desktop Services Licensing**

2. After selecting these components, the Remote Desktop Services Setup screen displays a choice of Remote Desktop Services modes. Select **Application Server mode**. This mode is recommended for Developer, because it means that client machines can only install programs using the Remote Desktop Services server (using Add/Remove Programs in the Windows Control Panel).

   Note: *To use Application Server mode, you must install a Remote Desktop Services licensing server in your domain within 90 days. Refer to Windows documentation for more information.*

3. Once the Remote Desktop Services mode has been selected, set the default permissions for application compatibility.

   Options available in Windows Server 2016

   - **Full Security**

     This option uses the latest Windows Server 2016 security features and provides the most secure environment for your Remote Desktop Services. However, some applications that were designed to run on earlier platforms might not run properly. You can use the Remote Desktop Services Configuration tool to relax security at any time if this option proves to be too restrictive.

   - **Relaxed Security**

     This option lessens many of the security enhancements in Windows Server 2016. Under this configuration, users have access to critical registry and system file locations. This might be necessary in order to run some applications that were designed for earlier platforms.

   The Developer installation is not affected by this option, so you should select an option based on the number of other legacy programs you are running, and the level of security required.

4. When you have selected your default permissions, continue with the standard Windows Server 2016 installation.

Creating Client Install Disks

Once Remote Desktop Services is installed on the server machine, create installation disks for the client machines.

To create the disks, perform the following:

1. Log in to the Remote Desktop Services server.
2. Select **Control Panel** > **Administrative Tools** > **Remote Desktop Services Client Creator**.
3. In the Create Installation Disk(s) dialog box, select Remote Desktop Services for 32-bit x86 windows. Click **OK** to finish creating the disks.

Use the created disks to install the Remote Desktop Services Client on your client machines.

Developer with Remote Desktop Services Installation and Configuration

To install Developer on the Remote Desktop Services server and to configure it for client use, perform the following:

1. Log in to the Remote Desktop Services server, then select **Programs and Features** from the Windows Control Panel.
2. Locate and open the Developer installation program (CDBrowser.exe) and click **Install**.

   Note: *If User Account Control setting is set to Always Notify, run the program as administrator.*
3. In the wizard dialog select the **All users begin with common application settings** option and click **Next** to start the Developer installation.
4. Select the **Custom Installation Type** and click **Next**.
5. In the Select Components dialog box, select only those components users need for a multiuser installation (for example, Developer). When complete, click **Next**.

   If required, the Version Control and Builder can be installed later.
6. Enter the following data in the Installation Configuration dialog box:
   - In the Installation Directory field, enter the location on the Remote Desktop Services server where Developer is to be installed.
   - In the Working Directory field, enter the path to the user’s Root Drive, for example, C:\Program Files (x86)\Unisys\AB Suite 7.0.
7. When the installation process is complete, click **OK**.
8. Return to the Programs and Features dialog box and choose **Next**, then **Finish**.
9. Restart the Remote Desktop Services server.

Note: *There should be separate copies of project and solution files for every user in the Remote Desktop Server and they should not be shared between the users.*

The Remote Desktop Services installation process is now complete.

Uninstalling Developer with Remote Desktop Services

To uninstall Developer, perform the following:

1. Select **Programs and Features** from the **Control Panel**.
2. Navigate to the Developer program folder, right-click and select **Uninstall**.
3. Click **Next** in the AB Suite Developer-InstallShield Wizard and select **Remove** and follow the Wizard.

Known Issues with Developer on Windows Remote Desktop Services

- Some issues might arise with auditing, changing management, and Version Control operations because on a Remote Desktop Services server installation, the machine name logged by Developer is the same for each user. To obtain usable audit information, it is recommended that Security is turned on so that both the user-id and machine name are logged.
- Each user can have multiple Remote Desktop Services server client sessions running, but should use a different username to log on to the Remote Desktop Services server to use Developer.
- The Remote Desktop Services server machine is generally not recommended for Primary or Backup Domain Controller.

Verifying Your Installation

To ensure your installation is correct, it is recommended that you create a new AB Suite project by using the sample AB Suite application or the sample AB Suite User Experience mode application from the templates provided in the New Project dialog box. You can then test the functionality with the sample model, create a build configuration, and then build and run the sample application.

Note: *The following verification steps are performed on the Windows platform.*

It is recommended to use the default Visual C# Development setting in Visual Studio for AB Suite Developer. This setting ensures that the entire shortcut keys work as expected in System Modeler. To set Visual C# Development Settings as a default setting in Visual Studio 2017, you must set or reset your profile.

Note: *A profile is a pre-defined settings collection you want to set the IDE to use.*

To set or reset your profile, perform the following:

1. On the **Tools** menu, select **Import and Export Settings**.
2. On Welcome to the Import and Export Settings Wizard page, click **Reset All Settings**, and then click **Next**.
3. On the Save Current Settings page, select **Yes, save my current settings**, and then click **Next**.
4. On the Choose a Default Collection of Settings page, select **Visual C# Development Settings** from the list, and then click **Finish**.

Creating an AB Suite Test Project

You can create an AB Suite test project by using the sample AB Suite application from the templates provided in the **New Project** dialog box for testing the functionality of the AB Suite Developer. You can then set the configuration properties, create a test database, build, and run the application.

To create an AB Suite project by using the sample AB Suite application, perform the following:

1. On the **File** menu, point to **New**, and then click **Project**.

   The **New Project** dialog box appears.
2. In the Project Types pane, expand **Templates**, expand **Agile Business Suite**, and then click **Samples**.
3. In the Templates pane, select **Sample Application**.
4. Click **Next**.

   The **Configure your new project** window appears.
5. In the **Name** box, enter the project name.
6. In the **Location** box, enter the path or browse to the location where you want to store the new project.
7. Click **OK**.

   The **New Application** Wizard appears.
8. From the **Server Name** list, select the SQL server. By default, this list box displays the system name.
9. In the **Database Name** box, enter the model name. By default, this test box displays the solution name.
10. In the **Model Name** box, enter the model name. By default, this text box displays the solution name.
11. Click **Next**.

    The project creation confirmation message appears in the wizard.
12. Click **Finish**.

    The sample AB Suite application is restored.
13. Click **Close**.

The AB Suite project is created in the specified location and the sample AB Suite model node appears in the Class View window.

Creating a Deployment Folder

The SAMPLE.model file contains a deployment folder with pre-defined configuration properties. If you are using a model file without a deployment folder you must perform the following:

1. Right-click the model node in the Class View window, point to **Add**, and then select **Folder** from the context menu.

   A folder with the default name "Folder1" is created under the model node. This folder can be used as a container for configuration properties.

2. Drag the segment into the deployment folder to apply these configuration properties to the segment.

   A newly created deployment folder contains default settings. These settings must be modified to allow the sample application to be deployed successfully.

3. Rename the deployment folder from "Folder1" to an appropriate name. For example, "SampleDeploy".

Configuring the Deployment Folder

You must configure the deployment folder before you build the application.

To configure the deployment folder, perform the following:

1. Right-click the deployment folder and select **Properties** from the context menu.

   The **<Deployment Folder Name> Property Pages** dialog box appears.

2. From the **Configuration** list, select **Release**.

3. From the **Platform** list, select **Windows**. By default, this property is set to **MCP**.

4. Under the **Build Target Filter** section, set the **Deployable** property to **True**.

   This enables the other configuration properties.

5. Under Builder Target Filter section, set the **Deploy Application Components**, **Deploy Database**, **Deploy Reports**, and **Deploy Winform User Interface** properties to **True**.

6. Under Installation section, set the **Deployment Host** property to "localhost" for local deployment (where Runtime and System Modeler are installed on the same physical machine).

7. Browse to and select the **Package Installation Directory** where the deployable unit should be installed on the runtime server. For example, "C:\Program Files (x86)\Unisys\AB Suite 7.0\Sample". This is the location of all executable files for the deployed system.

8. Browse to and select the **Package Intermediate Directory** where you want to store the temporary installation files. For example, "C:\NGENSystems\Temp".

9. Click **OK**.

Configuring the Segment

To configure the segment, perform the following:

1. Right-click the segment and select **Properties** from the context menu.

   The **<Segment Name> Property Pages** dialog box appears.

2. From the **Configuration** list, select **Release**.
3. From the **Platform** list, select **Windows**. By default, this property is set to **MCP**.
4. Set the **Database Name** to specify the runtime database name for the application. For example, "SAMPLEDB".
5. Set the **Database Server Registration** to specify the database server instance alias name defined in the Administration Tool. You can use a default instance named "default".

You must then create a runtime database (for example, "SAMPLEDB") by using the Runtime Administration Tool.

Creating a Runtime Test Database

To create a runtime test database, perform the following:

1. Point to and click the **Start** icon in the bottom-left corner of the screen.
2. Right-click a blank part of the **Start** screen and then select **All apps**. Select **Administration Tool** under **Agile Business Suite 7.0** or type **Administration Tool** on the desktop.

   The AdminTool window appears.

3. Right-click **Favorites** and select **Add Server…**.

   The **Add Server to Favorites** dialog box appears.

4. Enter the local server name in the **Server name** box.

   The server name appears under Favorites.

5. Expand the server you added and locate the "default" server registration node. If the "default" server registration node does not exist, perform the following:

   a. Right-click the server node, point to **All Tasks**, and then select **Register Database Server**.

      The **Register DB Server** dialog box appears.

   b. In the **DBMS registration** alias name box, enter "default".

   c. In the **Server machine** box, enter the name of your local server.

   d. In the **Instance name** box, enter the SQL named instance. If you are using a default instance.

   e. Click **OK**.

6. Right-click the "default" server node, point to **New**, and then select **Database…**, to add a new SQL Server database. For example, enter "SAMPLEDB" as the database name.

Note: *You must install SQL Server Management Studio (SSMS) and add the application administrative user to the MSSQL Server login as sysadmin before creating the runtime test database. If you do not perform this the authentication fails and you are prompted to add the application administrative user to the MSSQL Server login as sysadmin.*

Building the Application

To build the application, perform the following:

1. Open the Class View window and select the top-level deployment folder.
2. Right-click the deployment folder, and select **Build**.

You must enter the Application User Name and password to build the application. Refer to Preparing for Installation of Agile Business Suite for more information on setting up an administrator account. If deploying locally, enter the Domain as ".". The progress of the build operation appears in the Output window.

The build places all the deployed executable files in a series of sub-folders within the folder defined in the "Package Installation Directory" property. If this property is not defined, the executable files are stored in the default location, which is in a folder within the folder where the Agile Business Suite software is installed. For example, C:\Program Files (x86)\Unisys.

The contents of these folders are as follows:

- Database tables – The database tables are created within the SQL Server database.
- Winform dlls – The Winform dlls (one per ispec) can be located in

  ..\Sample\Interfaces\Winforms\Bin\<language number> within the folder structure.
- Application Component dll – The application component dll can be located in

  ..\Sample\Core\Bin.

The application is installed as a COM+ application.

Testing the Application

Refer to the *Agile Business Suite Developer User Guide* to run debugger and test that the application works correctly.

If you want to run the sample application by using the Winform client installed with AB Suite Developer, you must edit the ispec.xml file that is generated by the system. Refer to Configuring Winform for more information. The config.xml file is located at <Developer installation folder>\Unisys\AB Suite 7.0\Bin.

Creating an AB Suite Client Framework Test Project

You can create an AB Suite Client Framework test project by using the sample AB Suite User Experience mode application from the templates provided in the **New Project** window and test the functionality of the AB Suite Developer. You can then set the configuration properties, create a test database, build, and run the application

To create an AB Suite Client Framework test project by using the sample AB Suite User Experience mode application, perform the following

1. On the **File** menu, point to **New**, and then click **Project**.

   The **New Project** dialog box appears.

2. In the Project Types pane, expand **Agile Business Suite**, and then click **Samples**.
3. In the **Templates** pane, select **Sample User Experience mode Application**.
4. In the **Name** box, enter the project name.
5. In the **Location** box, enter the path or browse to the location where you want to store the new project.
6. Click **OK**.

   The **New Application** Wizard appears.

7. From the **Server Name** list, select the SQL server. By default, this list box displays the system name.
8. In the **Database Name** box, enter the model name. By default, this text box displays the solution name.
9. In the **Model Name** box, enter the model name. By default, this text box displays the solution name.
10. Click **Next**.

    The project creation confirmation message appears in the wizard.

11. Click **Finish**.

    The sample AB Suite User Experience mode model is restored.

12. Click **Close**.

A Client Framework project is created in the specified location and the model node appears in the Class view window.

After creating the AB Suite Client Framework project by using the sample AB Suite User Experience mode application, you might have to configure a deployment folder. The NewSampleSys.model contains a deployment folder with pre-defined configuration properties. Refer to Creating a Deployment Folder for more information on creating a deployment folder, if you are using a model file without a deployment folder.

Configuring the Deployment Folder

You must configure the deployment folder before you build the application.

To configure the deployment folder, perform the following:

1. Right-click the deployment folder and select **Properties** from the context menu.

   The **<Deployment Folder Name> Property Pages** dialog box appears.

2. From the **Configuration** list, select **Release**.
3. From the **Platform** list, select **Windows**. By default, this property is set to **MCP**.

4. Under the Build Target Filter section, set the **Deployable** property to **True**.

   This enables the other configuration properties.

5. Under Builder Target Filter section, set the **Deploy Application Components**, **Deploy Database**, and **Deploy Reports** properties to **True**.
6. Under Installation section, set the **Deployment Host** property to "localhost" for local deployment (where Runtime and System Modeler are installed on the same physical machine).
7. Browse to and select the **Package Installation Directory** where the deployable unit should be installed on the runtime server. For example, "C:\Program Files (x86)\Unisys\AB Suite 7.0\Sample". This is the location of all executable files for the deployed system.
8. Browse to and select the **Package Intermediate Directory** where you want to store the temporary installation files. For example, "C:\NGENSystems\Temp".
9. Click **OK**.

You can now perform the following:

1. Configure the segment
2. Create a runtime test database
3. Build the application

Refer to Creating an AB Suite Test Project for more information.

Testing the Client Framework Application

The sample Client Framework Model includes a set of designed XAML Views for the Sample system. You can use the supplied Views to test the deployed Client Framework application with the WPF Client.

To run the WPF Client against the AB Suite Client Framework application, you might have to edit the <Technology Folder Name>_Config.rtxml file. The configuration file is located at <System Modeler project folder>\Access Layer API Deploy. See Installing Client Framework for more information on the tags that you must edit in the <Technology Folder Name>_Config.rtxml file.

Verifying and Viewing Online Help

To verify if the AB Suite online help is installed and to view the help, perform the following:

1. Open Agile Business Suite 7.0 Development Environment.
2. If you have installed Help Viewer on your machine, perform the following:

   On the **Help** menu, point to **Set Help Preference**, and then select either of the following:

- **Launch in Browser** – Select this option if you want to view help in information center.
- **Launch in Help Viewer** – Select this option if you want to view help in help viewer.

The AB Suite online help appears in the Information Center or in the Microsoft Help Viewer depending on the preference you select. You can press F1 on the keyboard to view context specific information.

Notes:

- *The Set Help Preference option is visible only if you install Help Viewer.*
- *Help Viewer is not installed by default when you install Visual Studio 2017. You must select this component when you install Visual Studio 2017 or install it later from the Visual Studio Installer. Refer to MSDN documentation for more information on installing Microsoft Help Viewer.*

If you have not installed Help Viewer on your machine, perform the following:

On the **Help** menu, click **View Help**.

The AB Suite online help appears in the Information Center or in the Microsoft Help Viewer depending on the preference you select. You can press **F1** on the keyboard to view context specific information.

Known Issues with Windows Server 2016

When Developer is installed on Windows Server 2016, help viewer displays HTML text as MIME Sniffing is disabled in the security settings of Internet Explorer, by default.

Workaround

To display Developer online help in the help viewer, perform the following after closing help viewer:

1. In Internet Explorer, click **Internet Options** on the **Tools** menu or select **Tools** button, and then select Internet options.

   The **Internet Options** dialog box appears.

2. Select the **Security** tab and click **Custom level...**.
3. In the **Security Settings - Internet Zone** dialog box, select **Enable** for **Enable MIME Sniffing** in **Miscellaneous** section.
4. Click **OK** to close Security Settings - Internet Zone dialog box.
5. Click **OK** to close Internet Options dialog box.

   Open help viewer to check if help appears.

If the following warning appears, turn off the IE enhanced security configuration:

Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.

https://docs.microsoft.com

To turn off the IE enhanced security configuration, perform the following:

1. Open Server Manager.
2. In the left pane, select **Local Server**.

   The right pane displays the IE Enhanced Security Configuration option. By default this option is set to On.
3. Click **On**.

   The Internet Explorer Enhanced Security Configuration windows appears.
4. Select **Off** under **Administrators**.
5. Select **Off** under **Users**.
6. Click **OK**.

When you view the AB Suite online help in the Information center, an Application Error appears.

Workaround

If the Application Error appears, you must add the Product Support Site to Trusted sites in the Internet security settings of the Internet Explorer.

To add the Product Support Site to Trusted site, perform the following:

1. Open Internet Options.
2. On the **Security** tab, select **Trusted sites**, and then click **Sites**.

   The Trusted sites window appears.
3. In the **Add this website to the zone** box, enter the following Product Support Site link:

   https://www.support.unisys.com
4. Click **Add**, and then click **Close**.
5. Click **OK**.

Uninstalling or Repairing the AB Suite Developer

You can uninstall or repair the Developer installation from the Programs and Features option in the Control Panel.

Note: *If you want to uninstall Visual Studio, you must first uninstall AB Suite Developer, otherwise fragments of AB Suite Developer might be left after Visual Studio is uninstalled, and might cause problems with future installations.*

To uninstall or repair the AB Suite Developer, perform the following

1. Open **Programs and Features** from **Control Panel**.
2. Right-click **Agile Business Suite 7.0 Developer** from the list, and select **Uninstall or Repair**.

Notes:

- *If you select the* ***Uninstall*** *option, click "Yes" or "No" when prompted to confirm and continue with the operation.*
- *If you select the* ***Repair*** *option, the installation proceeds normally and all installation errors are fixed by reinstalling all non-customizable files in the same location as the previous installation. If any of the files were accidentally deleted or modified, this option restores the software to its original state. You can use the* ***Repair*** *option by double-clicking Setup.exe and the installation runs in maintenance mode. If you try to repair the Developer installation from*
    - *Control Panel, Programs and Features option, the repair operation executes in silent mode.*
    - *Setup.exe, you are prompted with the Application User and Application Administrative User maintenance mode dialog boxes.*

      During repair of the Development installation, some files are not restored automatically as they are not part of the Windows Installer. You can manually copy these files from the Development Environment folder of the Developer installer, if required. The following are the list of files that can be manually copied:

        - config.xml
        - readme.htm
        - ROC18CE.jar
        - ROCCLR.model

Uninstalling and Reinstalling AB Suite

To uninstall AB Suite, you must delete all runtime systems. The COM+ settings might be lost when the runtime systems are deleted. Refer to Uninstall Agile Business Suite Runtime for more information.

A utility, AB Suite COM+ Migrator (ABSCOMMigrator.exe) is provided to save and restore the Pooling and Activation settings after the rebuild of the user systems. You can find the ABSComPlusMigrator.exe in the AB Suite Runtime installer, CD Runtime\Windows Runtime\Runtime Utilities.

For an AB Suite Generated COM+ application, both Pooling settings and User Role information can be backed up and restored through this utility. For AB Suite Runtime internal COM+ Settings, only User Role information can be backed up and restored through this utility.

Note: *Ensure that you use ABSCOMMigrator.exe to save and restore the Pooling and Activation settings.*

Backing up and Restoring

Prior to uninstalling AB Suite, you might take a backup of the Pooling settings and User Role information through the AB Suite COM+ Migrator utility. The backup is stored in XML format with a file name specified by you. After reinstalling AB Suite at the desired IC level, you must execute the AB Suite COM+ Migrator utility to restore the settings of the COM+ application.

Each backup file settings include Pooling settings, Activation settings and User Role settings.

1. Following is the list of the Pooling settings for an AB Suite generated COM+ application that can be backed up and restored.
   - Pool Size
   - Lifetime Limit (minutes)
   - Memory Limit (KB)
   - Expiration Timeout (minutes)
   - Call Limit
   - Activation Limit
2. Following is the list of the Activation settings for an AB Suite generated COM+ application that can be backed up and restored.
   - Minimum Pool Size
   - Maximum Pool Size
   - Creation Timeout (ms)
3. User Role settings for an AB Suite runtime application and AB Suite generated COM+ application can be backed up and restored.

Following is the list of the AB Suite Runtime internal COM+ applications that can be backed up and restored.

- Database Manager
- DB Reorganisation
- Debugger Manager
- Deployment Server
- External Call Helper
- Hub Helper
- Hub Transaction Context
- Hub Transaction Co-ordinator
- Print Configuration Manager
- Report Session Manager
- Runtime Manager

- Runtime Versioning
- Security Helper
- Segment Session Manager
- System Privileged

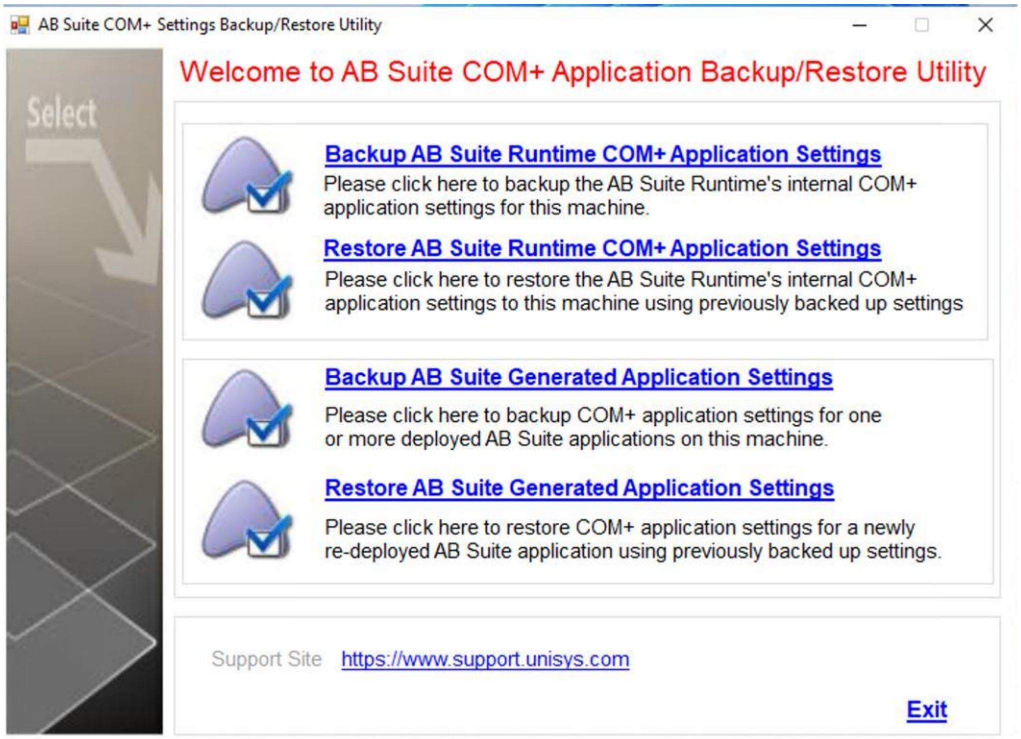
Using AB Suite COM+ Migrator Utility

The AB Suite COM+ Migrator utility enables you to select a link from the following list:

- Backup AB Suite Runtime COM+ Application Settings – Refer to Backup AB Suite Runtime COM+ Application Settings to back up AB Suite Runtime's internal COM+ application settings.
- Restore AB Suite Runtime COM+ Application Settings – Refer to Restore AB Suite Runtime COM+ Application Settings to restore AB Suite Runtime internal COM+ application settings.
- Backup AB Suite Generated Application Settings – Refer to Backup AB Suite Generated Application Settings to back up COM+ application settings for one or more deployed AB Suite applications.
- Restore AB Suite Generated Application Settings – Refer to Restore AB Suite Generated Application Settings to restore COM+ application settings for a newly re-deployed AB Suite application.

Note:

- *After executing the AB Suite COM+ Migrator utility, corresponding success or failure message is displayed.*



AB Suite COM+ Settings Backup/Restore Utility

Welcome to AB Suite COM+ Application Backup/Restore Utility

Backup AB Suite Runtime COM+ Application Settings
Please click here to backup the AB Suite Runtime's internal COM+ application settings for this machine.

Restore AB Suite Runtime COM+ Application Settings
Please click here to restore the AB Suite Runtime's internal COM+ application settings to this machine using previously backed up settings

Backup AB Suite Generated Application Settings
Please click here to backup COM+ application settings for one or more deployed AB Suite applications on this machine.

Restore AB Suite Generated Application Settings
Please click here to restore COM+ application settings for a newly re-deployed AB Suite application using previously backed up settings.

Support Site https://www.support.unisys.com

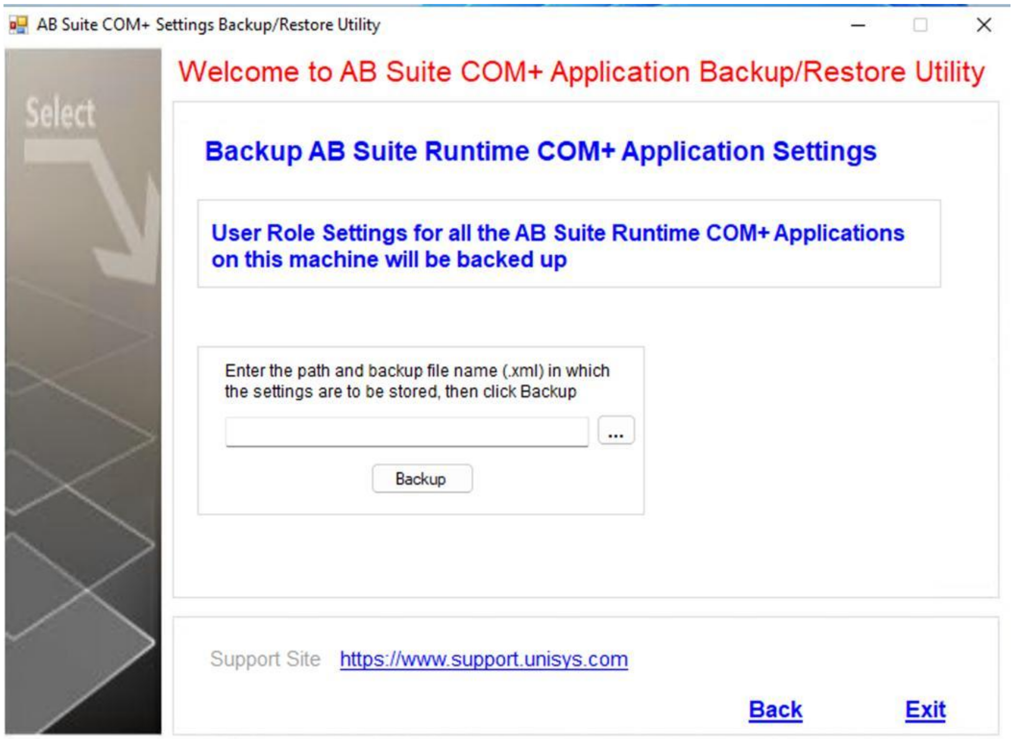
102222

Backup AB Suite Runtime COM+ Application Settings

This link enables you to back up the User Role settings.

To back up User Role settings, perform the following:

1. Select the path and specify the backup file name (.xml)
2. Click **Backup** to back up the internal COM+ application settings.



AB Suite COM+ Settings Backup/Restore Utility

Welcome to AB Suite COM+ Application Backup/Restore Utility

Backup AB Suite Runtime COM+ Application Settings

User Role Settings for all the AB Suite Runtime COM+ Applications on this machine will be backed up

Enter the path and backup file name (.xml) in which the settings are to be stored, then click Backup

Support Site https://www.support.unisys.com

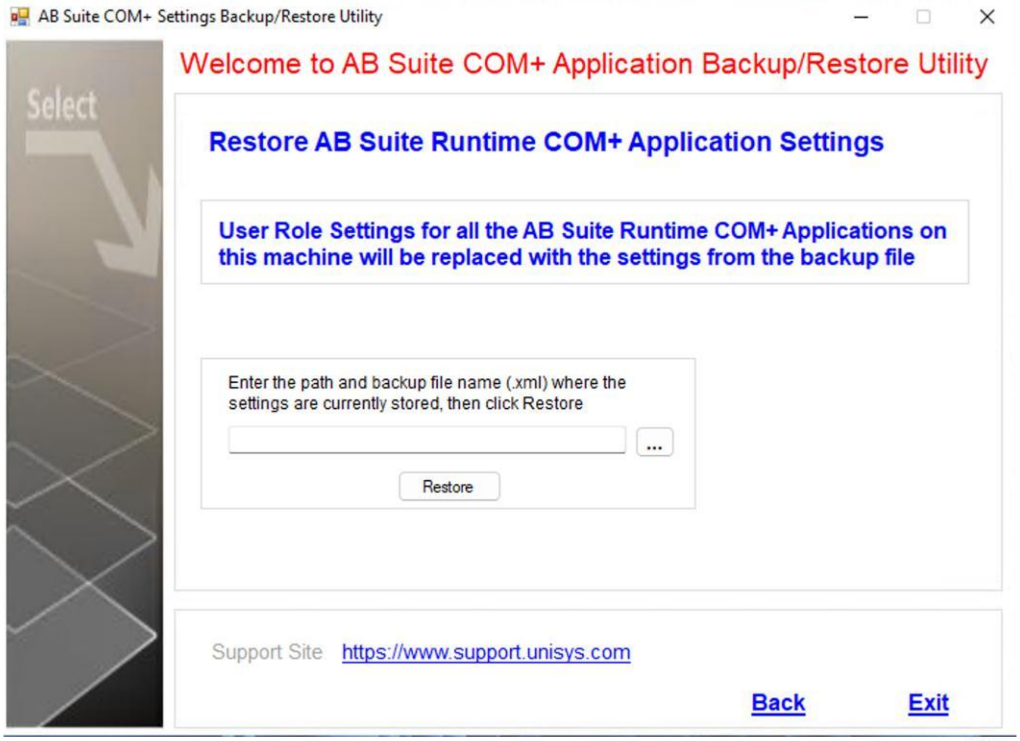
102223

Restore AB Suite Runtime COM+ Application Settings

This link enables you to restore the User Role settings to the machine by using the previously backed up settings for an application.

To restore User Role settings, perform the following:

1. Select the path and backup file name (.xml) from where the AB Suite runtime COM+ application settings can be restored.
2. Click **Restore** to restore the AB Suite runtime COM+ application settings.


AB Suite COM+ Settings Backup/Restore Utility
Select
Welcome to AB Suite COM+ Application Backup/Restore Utility
...
Restore
Back
Exit

Restore AB Suite Runtime COM+ Application Settings

User Role Settings for all the AB Suite Runtime COM+ Applications on this machine will be replaced with the settings from the backup file

Enter the path and backup file name (.xml) where the settings are currently stored, then click Restore

Support Site https://www.support.unisys.com

102226

Backup AB Suite Generated Application Settings

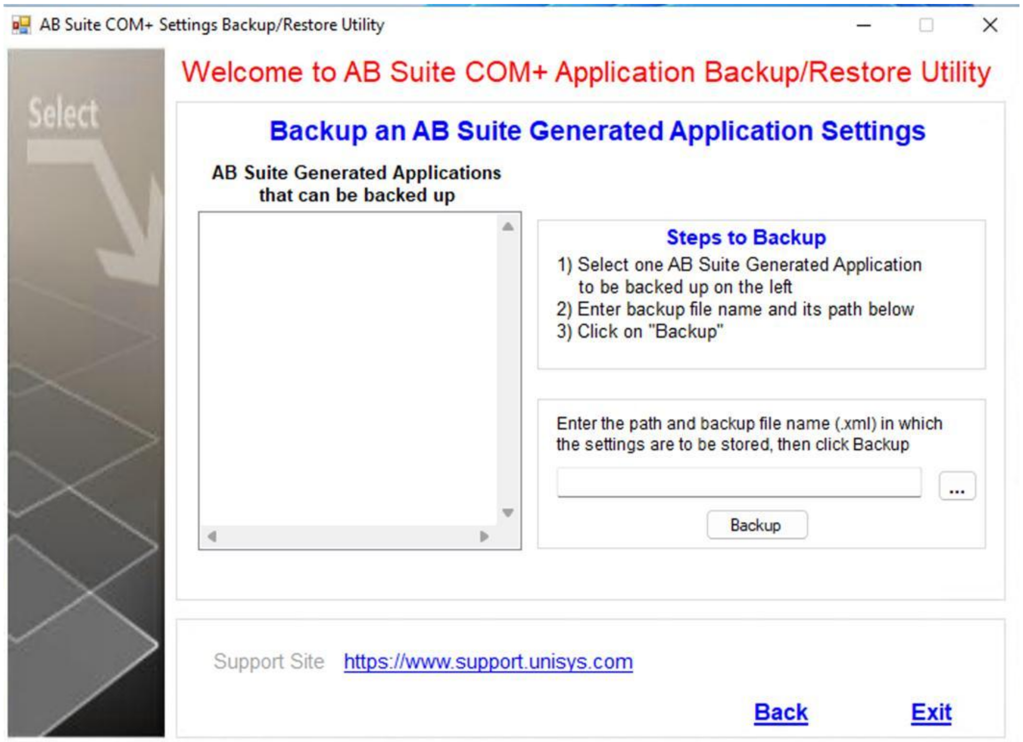
This link enables you to back up Activation settings, Pooling settings, and User Role settings for one or more deployed AB Suite applications on the machine.

1. Select the AB Suite generated application that needs to be backed up from the list of applications available in the AB Suite Generated Applications that can be backed up list box.

   Note: *The utility lists all the AB Suite generated COM+ applications. You can select the application to be backed up.*

2. Select the path and specify the backup file name (.xml)

3. Click **Backup** to back up an AB Suite generated application's settings.



AB Suite COM+ Settings Backup/Restore Utility
Select
Welcome to AB Suite COM+ Application Backup/Restore Utility
Backup an AB Suite Generated Application Settings
AB Suite Generated Applications that can be backed up

Steps to Backup
1) Select one AB Suite Generated Application to be backed up on the left
2) Enter backup file name and its path below
3) Click on "Backup"

Enter the path and backup file name (.xml) in which the settings are to be stored, then click Backup

...
Backup
Support Site
https://www.support.unisys.com
Back
Exit

102225

Restore AB Suite Generated Application Settings

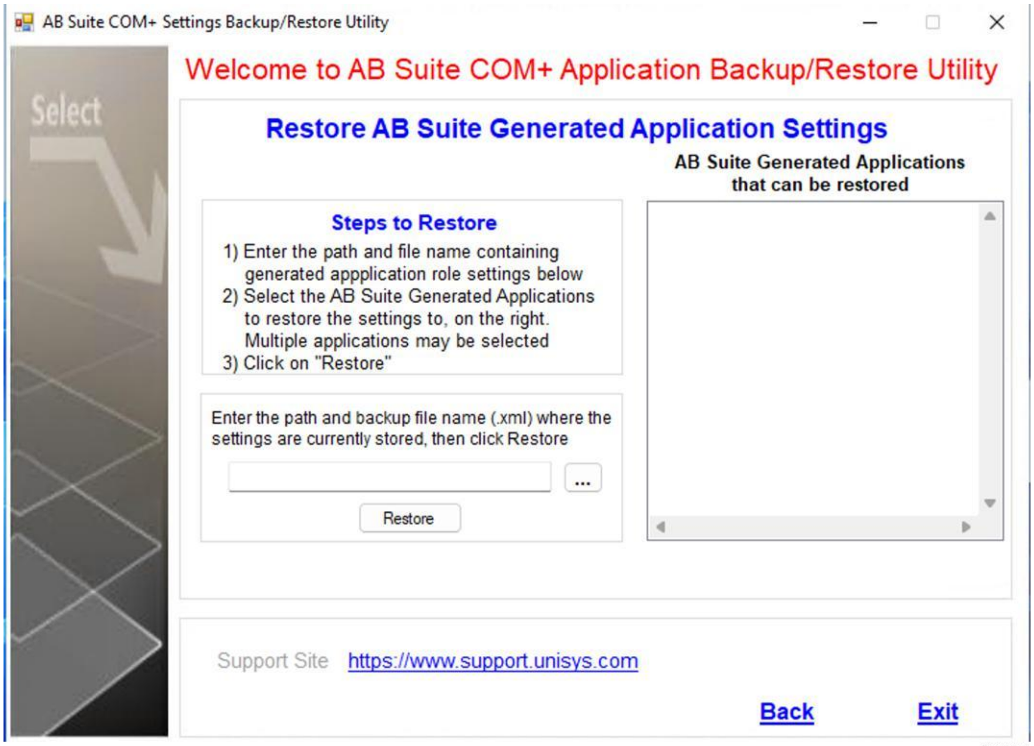
This link restores Activation settings, Pooling settings, and User Role settings for a newly re-deployed AB Suite application by using the previously backed up settings.

1. Select the path and backup file name, where the settings of the previously backed up application are stored.

2. Select the AB suite generated applications to be restored from the **AB Suite Generated Applications that can be restored** list box.

   Note: *A backup file’s settings (Pooling settings, Activation settings, and User Role settings) can be applied to multiple AB Suite applications.*

3. Click **Restore** to restore the AB Suite generated application’s settings.



Welcome to AB Suite COM+ Application Backup/Restore Utility

Restore AB Suite Generated Application Settings

AB Suite Generated Applications that can be restored

Steps to Restore

1) Enter the path and file name containing generated appplication role settings below
2) Select the AB Suite Generated Applications to restore the settings to, on the right. Multiple applications may be selected
3) Click on "Restore"

Enter the path and backup file name (.xml) where the settings are currently stored, then click Restore

Support Site https://www.support.unisys.com

102224

Using Command Line Options

Use the following command statement to back up and restore the Pooling settings and User Role information.

```
ABSComPlusMigrator.exe [-B|-R] [-S (Com Application name)|-N]
[-X (xml file path)] [-L (log file path)]
```

Note: *You can find the ABSComPlusMigrator.exe in the AB Suite Runtime installer, CD Runtime\Windows Runtime\Runtime Utilities.*

Where:

Syntax	Description
-B	To back up the properties of ComApplication
-R	To restore the properties of ComApplication
-S (Com Application name)	To specify the AB Suite generated ComApplication name
-N	To specify AB Suite's Runtime ComApplications.
-X (xml file path)	The name of the Xml File path (Fully qualified path)

Syntax	Description
-L (log file path)	The name of the log file (Fully qualified path - Optional; if not specified, log file with name ABSComMigrator.log is created in the location "Data\public\log")
/? or -Help	Lists Help details

Examples for using command line options

This section provides examples on using the command statement.

Examples	Command Statement	Description
To back up ABSuite Generated System's ComApplication, SAMPLECLR	ABSComPlusMigrator.exe -B -S SAMPLECLR -X "c:\SampleClrBackup.xm" -L "c:\SampleClrBackup.log"	- SAMPLECLR: Generated Com Application name - c:\SampleClrBackup.xml: Fully qualified xml file path. - c:\SampleClrBackup.log: Fully qualified log file path (optional).
To back up ABSuite's Runtime ComApplications	ABSComPlusMigrator.exe -B -N -X "c:\NGENComApplicationsBackup.xml" -L "c:\NGENComApplicationsBackup.log"	- c:\NGENComApplicationsBackup.xml: Fully qualified xml file path - c:\NGENComApplicationsBackup.log: Fully qualified log file path (optional).
To restore ABSuite Generated System's ComApplication, SAMPLECLR	ABSComPlusMigrator.exe -R -S SAMPLECLR -X "c:\SampleClrBackup.xml" -L "c:\SampleClrRestore.log"	- SAMPLECLR: Generated Com Application name - c:\SampleClrBackup.xml: Fully qualified xml file path. - c:\SampleClrRestore.log: Fully qualified log file path (optional) ***Note:*** *One backup file settings (Pooling settings, Activation settings, and User Role settings) can be applied only to one AB Suite application.*

Examples	Command Statement	Description
To restore ABSuite’s Runtime ComApplications	ABSComPlusMigrator.exe -R -N X”c:\NGENComApplicationsBackup.xml” -L “ c:\NGENComApplicationsRestore.log”	• c:\NGENComApplicationsBackup.xml: Fully qualified xml file path. • c:\NGENComApplicationsBackup.xml: Fully qualified xml file path.
To restore properties of ComApplication, SAMPLECLR to ComApplication, CHOCSYSCLR	ABSComPlusMigrator.exe -R -S CHOCSYSCLR -X “c:\SampleClrBackup.xml” -L “c:\ChocsysClrBackup.log”	• CHOCSYSCLR: Com Application name • c:\SampleClrBackup.xml: Fully qualified xml file path • c:\ChocsysClrBackup.log : Fully qualified log file path (optional)

Enabling LargeAddressAware option for Agile Business Suite in Windows

32-bit processes under Windows are limited to address 2 GB memory. However, you can use the 4-gigabyte tuning (4GT) feature on Windows to increase the memory up to 3 GB. You can then use the /LARGEADDRESSAWARE switch to enable AB Suite to use the large address space.

To use the 4GT feature and the /LARGEADDRESSAWARE switch for increasing the memory, perform the following:

1. Enable 4GT using the BCDEdit /set *increaseuserva* command.

   You can set the *increaseuserva* option to a value between 2048 (2 GB) and 3072 (3 GB).

2. Open command line.

3. Browse to the folder where devenv.exe is installed.

   For example, if you have installed Visual Studio 2017 on C drive, you can locate the devenv.exe in the following location:

   C:\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\IDE

4. Type the command editbin /LARGEADDRESSAWARE devenv.exe to enable AB Suite to use the large address space.

Section 4
Developer Configuration

Configure Debugger for Normal Users

This section discusses how to configure AB Suite Debugger so normal users without administrative privileges can debug AB Suite systems. AB Suite internally uses the user group called Debugger Users on the local machine to allow non-administrative users' access to Debugger. The install creates this user group if it does not already exist.

File Permissions for Builder Output and Cache Directories

The following directories need full read and write access by the Debugger Users group. If necessary, you can change the location of the Builder Output and Cache directories through the System Modeler Builder options to use a shared location.

1. Builder Output Directory
2. Cache Directory

The Debugger Users group needs Full Control access on the Builder Output and Cache directories. In order to do this, perform the following:

1. Browse to the location of the Builder Output directory.
2. Right-click the **Builder Output directory**, and select **Properties**. The **Builder Output Properties** dialog box is displayed.
3. Select the **Security** tab, and select the Debugger Users in the Group or user names pane.
4. Select the **Allow Full Control** check box in the Permissions for Debugger users.
5. Click **Apply** and **OK**.

Refer to Changing Builder Output and Cache Directories for more information on changing the directory locations.

File Permissions for Existing Data Folder

The existing files under the following directories need full read and write permissions for the Debugger Users group.

1. AB Suite 7.0\Data\Private
2. AB Suite 7.0\Data\Public

The Debugger Users group need Read, Write, and Modify access on the existing files under AB Suite 7.0\Data\Private and AB Suite 7.0\Data\Public. To assign the access rights to the debugger group, perform the following:

1. Browse to the location of the Builder Output directory.
2. Right-click the Builder Output directory, and select **Properties**.

   The **Builder Output Properties** dialog box is displayed.
3. Select the **Security** tab, and select the Debugger Users in the Group or user names pane.
4. Click **Edit**.
5. Select the **Read, Write, and Modify** check box in the Permissions for Debugger users dialog box.
6. Click **Apply** and **OK**.

Adding New Non-administrative User Access to Debugger

To allow a new non-administrative user access to AB Suite Debugger, an administrator needs to add the user to the Debugger Users group and give appropriate database permissions:

1. Add the new or existing user to the Debugger Users group.
2. Set appropriate database permissions for this user or for all Debugger Users to be able to access the model database. Follow instructions mentioned in the Database Permissions needed subsection.
3. The user can now use Debugger and Debugger Administration applications.

Notes:

- *Debugger Users cannot access the Runtime Administration Tool. If Debugger users need a new debugger runtime database, then an Administrator should create their runtime database in the Runtime Administration Tool for them.*
- *Debugger Users must add a set of translation libraries specific to the encoding used for EAE OS 2200 when using external classes targeting Kanji data. These libraries are the same as those used by EAE Developer. As the internal code mappings of the Japanese character set are different for the LETS-J code (on OS 2200) and the Shift JIS code (on Windows), you must add the following libraries to the <AB Suite Installation Path>\Bin folder. For example:"C:\Program Files(x86)\Unisys\AB Suite 7.0\Bin" in 64-bit operating system:*
  - *mcutil.dll*
  - *mcletsj.dll*
  - *mbcsconv.dll*

- *eudcserv.dll AB Suite 7.0 does not support 32–bit operating systems.*

Changing Builder Output and Cache Directories

The Builder Output and Cache Directory Locations should be in a shared directory location. This ensures that all normal Debugger users without administrative privileges can access the model database.

To change the Builder Output and Cache directories, perform the following:

1. Log on as an administrator.
2. Launch **Microsoft Visual Studio 2017**.
3. Select **Options** from the Tools menu.
4. Navigate to System Modeler, and then Builder.
5. Change the Location of Cache and Builder Output to a shared directory location that all users can access.

Database Permissions Needed

Create new model databases (optional)

This permission is required if a debugger user without administrative rights wishes to use AB Suite to create new models.

1. Log on as an administrator of the computer.
2. Launch **Microsoft SQL Server Management Studio**.
3. Navigate to Security and then Logins.
4. Add the debugger user as a new login. You can either add the individual user or the Debugger Users group. Adding the Debugger Users group is recommended if all your users can access the same databases.
5. Right-click or double-click to view the properties on the added user.
6. Choose Server roles and check dbcreator. This allows the user to create new databases when creating a new AB Suite model.

Accessing existing model databases (required)

This permission is required for debugger users without administrative rights who want to use existing AB Suite model databases.

1. Log on as an administrator to the computer.
2. Launch **Microsoft SQL Server Management Studio**.
3. Navigate to Security and then Logins.
4. Right-click on the Login node and select **New Login**. Add the debugger user as a

new login. You can either add the individual user or the Debugger Users group. Adding the Debugger Users group is recommended if all your users can access the same databases.

5. Ensure Windows authentication is selected.
6. Choose User Mapping and select the model database that the user needs access to.

Runtime databases for debugging

Without Administrative rights, Debugger Users cannot access the Runtime Administration Tool to create and delete runtime databases. If your Debugger users need a new debugger runtime database, then an Administrator should create their runtime database in the Administration tool for them.

Configure Debugger for Remote Desktop Users

To configure Debugger for Remote Desktop users, follow the same procedure as required for normal users, but the configuration properties for each remote user should be different. Since, each remote user needs to create their own configuration in the model with unique property values. Ensure to specify unique values for the Segment configuration properties; COM Prog ID, Alternate Name, and DB Schema Name.

Section 5
Client Environment Installation

This section describes how to install the Agile Business Suite Client Environment.

Required System Software

This section describes the software required for Component Enabler and Client Framework. Depending on how you use Component Enabler and Client Framework, you might require some or all of the following components:

- Windows 10 Enterprise, Professional (x64) October 2018 Update, Windows Server 2016 Standard, Datacenter, or Windows Server 2019 Standard, DataCenter
- Agile Business Suite Developer and Builder
- Web server
- Remote Access server
- Agile Business Suite Runtime

The system requirements vary, depending on how you plan to access the Client Environment applications. Any differences in system requirements are noted for each component. There might also be additional requirements for individual components, in which case they are specified in the relevant section.

Generation Workstation

The development and generation workstation for Component Enabler requires the following software:

- Agile Business Suite Developer and Builder, to generate classes from the system definitions stored in the Developer Model database.
- Microsoft Visual Studio 2017 Professional version 15.9.7 or later – enhance the generated applications for .NET, such as ASP.NET Web Forms, ASP.NET Web Services and the VB.NET Client).
- A Development Environment of choice, if you are developing your own applications to access the Component Enabler client interface.

When using the Java Generate Environment:

- Oracle Java® Plug-in Version 1.6 or later.

  Note: *Java 1.8 is supported, except for custom generators. Java 1.6 or later is required (including custom generators).*

For the Microsoft .NET based Generate Environment:

- Microsoft .NET Framework 4.7.2 or later.

  When generating Java based applications, you need the Java Software Development Kit v1.6 or later. When generating for Microsoft .NET based applications, you need the C# compiler installed on the machine.

The developer workstation for the Client Framework requires the following software:

- Agile Business Suite Developer and Builder
- The development environment for the technology of choice; for example, Microsoft Visual Studio 2017 to develop applications by using technologies, such as WPF/XAML, ASP.NET MVC (Model-View-Controller), Windows Communication Foundation (WCF), and Windows Store Apps
- Microsoft .NET Framework 4.7.2 or later

Note: *If you are developing Windows Store Apps by using Client Framework, you must install AB Suite Developer on Windows 10 or later operating system.*

Client Workstation

The Component Enabler client workstation is the workstation through which users access Component Enabler applications. You need the following software on your client workstation:

Notes:

- *These applications do not require the JDK or the C# compiler on the client workstation.*
- *For Java applications that use Component Enabler, you need a Java Virtual Machine, such as the Oracle Java Runtime Environment, Version 1.6 or later .*
- For applications that use the Component Enabler for .NET interface, you need:
  - The Microsoft .NET Framework 4.7.2 or later.

  You do not need a Web browser.
- When running the Presentation Client as a standalone application, or the JSP Client, you need:
  - An operating system with TCP/IP services installed, for example, Windows 10 Enterprise (x64) Professional, Enterprise (x64) October 2018 Update or Mac OS X.
  - A Java 1.6 or higher Virtual Machine (JVM), such as the one supplied by Oracle.
- When running the Presentation Client from a Web browser, you need:

  - An operating system with TCP/IP services installed; for example, Windows 10 Enterprise (x64), Professional (x64) October 2018 Update or Mac OS X.
  - One of the following qualified browsers:

    Microsoft Internet Explorer 11.0 or later

    FireFox or later

    Safari (for MAC OS X)
  - Java version 1.6 or later, compatible plug-in.

Note: *These applications do not require the JDK on the client workstation.*

- For applications that use scripted pages on a Web server, you need an operating system with TCP/IP services installed; for example, Windows 10 Enterprise (x64) Professional, Enterprise (x64) October 2018 or UNIX®.

Remote Access Server

To communicate with a Component Enabler client, you need the following software on the server for the host system:

- Agile Business Suite Runtime
- TCP/IP
- Remote Access Server software

Note: *After the Remote Access server software is installed, you need to create Component Enabler Views before using the Remote Access servers to access the system. Refer to the Agile Business Suite Runtime Administration Guide for your host platform for more information.*

The Client Framework client workstation might be an end-user workstation or a server machine. A new connection mechanism, Access Layer API, is available in the Client Framework for connecting a client to the runtime system. The Access Layer API allows the client application to interact with the deployed AB Suite system and is exposed through Direct and Remote connection.

For direct connections, the client workstation requires the following software:

- .NET Framework 4.7.2 or later
- Access Layer API assemblies
- Data Models assembly for an application
- Application specific components. For example,
  - Data View Models and Views assemblies for a WPF Client application
  - Any dependent software required by the client technology that was used to develop the client application such as custom WPF Toolkit

Client Framework WCF Gateway Services

To remotely access the runtime system for Client Framework applications, the following AB Suite WCF gateway services are installed:

- AB Suite 7.0 Client Framework (WCF) FileStore Gateway – Allows Client Framework clients to retrieve or store files, such as images.
- AB Suite 7.0 Client Framework (WCF) Gateway – Allows Client Framework to access an AB Suite System over TCP/IP.

These services are installed when you install the AB Suite Runtime for Windows, and client applications can use them to interact with the deployed AB Suite runtime system.

For Developers, the Client Framework WCF Gateway Host application is also installed with the AB Suite Developer for Windows software. This is a WCF Service hosting application that can be used to test the WCF Gateway services on a machine where the AB Suite Runtime software is not installed. Refer to the *Agile Business Suite Developer User Guide* for more information on the WCF Gateway Host.

WCF follows a client-server model to establish communication between applications. The AB Suite WCF gateway can be

- Self-hosted in any managed .NET application
- Hosted as a Windows service
- Hosted in different versions of Internet Information Services (IIS)

Refer to the *MSDN documentation* for more information on hosting and consuming WCF services.

The remote Access Layer API uses .Net Portable Library assemblies. It can be used wherever portable libraries are required. For example, Windows 8 Store Apps, Silverlight , and Windows Phone 8 clients.

To enable Client Framework applications to connect to the runtime system remotely, the client workstation requires the following:

- .Net Framework Portable subset
- Access Layer API Remote assemblies
- .Net Portable DataModels for the application
- Application specific components. For example,
  - DataViewModels and Views assemblies for a SilverLight client application.
  - Any dependent software required by the client technology that was used to develop the client application, such as custom Silverlight Toolkit.
- The WCF Gateway server requires the following:
  - .Net Framework 4.7.2 or later
  - Access Layer API assemblies
  - .Net DataModels for an application

To configure the WCF Gateway, you must modify its associated configuration file, Unisys.ABSuite.AccessLayer.GatewayServiceLibrary.dll.config, which is installed in the Bin folder of the AB Suite installation directory.

Refer to the *MSDN documentation* for more information on configuring WCF Services and the options you can specify in the configuration file.

Client Framework Custom Service Libraries

If you have developed a custom WCF Service by using the Client Framework WCF Service technology option, you can install the associated WCF Hosting application as a Windows Service to host your Service Library.

You can install the associated WCF Hosting application as a Windows Service by running the following command from the command prompt:

```
InstallUtil <SegmentName>.<FolderName>Gateway.exe
```

To run the WCF Service with a specified user name and password, you must run the following command from the command prompt:

```
InstallUtil /user=<username> /password=<myPassword>
<SegmentName>.<FolderName>Gateway.exe
```

Notes:

- *You can run the WCF Service by using the Application User account. Alternatively, you can use a credential that has similar rights as the Application User.*
- *If you do not specify a user name and password, the WCF service runs as a local service.*

Refer to the *Agile Business Suite Developer User Guide* for more information on creating a custom service library.

To configure the custom service library for your WCF Hosting application, you must modify the necessary tags in the app.config file. The app.config file is created on the generation of the service library project.

When you host this gateway you can find the app.config file in the Solution Explorer window under WcfServiceLibrary project.

Refer to the *MSDN documentation* for more information on configuring the WCF gateway.

Minimum Hardware Requirements

This section describes the minimum recommended hardware requirements for installing Agile Business Suite Client Environment.

Hardware	Runtime
Processor	2 core, 2 GHz CPU
Memory	4 GB RAM
Disk space	200 GB
Monitor	LCD

Installing the Client Environment

To install Client Environment you must click Client Environment on the Unisys Installation Interface.

This displays the Client Environment interface. Note that the following installation options are selectable for installation on a development machine or on a client machine of the user.

From this interface, you can select the Client Environment that you want to install by clicking the appropriate button. The options are:

- Winform – installs either Winform 32-bit or Winform 64-bit software on a client machine depending on the operating system. You do not need to install this component if you have already installed the Development Environment, as the Winform container is included in that installation.
- Component Enabler – installs the Component Enabler software on a development machine.
- Presentation Client – installs the Presentation Client on a client machine. You do not need to install this component if you have already installed Component Enabler, as the Presentation Client is included in that installation.
- Business Integrator – installs the Business Integrator and associated product information on a development machine for generation with Component Enabler.
- Client Framework – installs the standalone Client Framework on a client machine. You do not need to install this component if you have already installed the Development Environment, as the Client Framework software is included in that installation.

Installing Winform

Before you install the Winform software, you must install the following software:

- Windows 10 Professional (x64), Enterprise (x64), Windows Server 2019 Standard, Datacenter, or Windows Server 2016 Standard, DataCenter
- .NET Framework 4.7.2 or later

You must also have administrative privileges on the machine on which you want to install Winforms, and 5Mb of free disk space.

Note: *For the Winform client machines to communicate with the runtime server, the usercodes of the client machines must be known on the server. This is accomplished when a user logs in by using a domain usercode/password, and that domain is trusted on the server. The Winform client machines cannot communicate with the runtime server if they are across non-trusted domains.*

You can install Winform (32-bit) or (64-bit) software on a client machine. You do not need to install this component if you have already installed the Development Environment, as the Winform container is included in that installation.

Click **Winform (32-bit)** or **Winform (64-bit)** to begin the installation. The Installation wizard appears and a number of checks are carried out on the system to ensure it has the correct underlying system software to complete a satisfactory installation. If the checks identify that a copy of Developer is installed on the machine, the Winform installation does not proceed, as the Developer installation includes the Winform software, which is required for the debugger functionality.

Note: *If two instances of the installation wizard appear, close one instance.*

If the checks indicate that the Winform software is already installed on the machine as a separate instance, the Repair Remove dialog box appears.

If the checks are successful, a welcome dialog box appears, followed by a license dialog box. Click **Yes** on the license dialog box, if you want to accept the conditions and continue with the installation.

You can then select the target drive and directory for the installation, if you do not want to accept the default installation location.

Note: *If an installation of Agile Business Suite Runtime exists on the target machine, the destination dialog is skipped, as the Winform software must be installed in the same location as the existing Runtime components.*

When you have entered the location for the target drive and directory, or accepted the default location for the installation, click **Next** to display the Start Copying Files dialog box. This allows you to review the installation settings before completing the installation. This screen displays components that are selected and the installation directory. If you are satisfied with the settings, click **Next** to proceed with the installation. You can click **Back** to make changes, if any.

At the completion of installation, the Installation Complete Screen appears. This screen allows you to view the readme file. If you do not want to view the readme file, clear the check box. Click **Finish** to complete the installation.

Configuring Winform

Before running applications, you must edit a configuration file named config.xml. This is an xml file that contains configuration information to enable the Winform clients to find and connect to the application component. This file is automatically created by the generation of the system. The administrator might have already modified this configuration file in the installation package. Check with your administrator before proceeding.

A default copy of config.xml file is located at <AB Suite installation folder>\Unisys\<AB Suite>\Bin.

Alternatively, a pre-configured version of this Winform configuration file, named ispec.xml is automatically generated each time a system is built with Builder. This file is located in the systems installation Bin folder.

For example:

```
C:\Sample\Release_Windows\SAMPLE\Core\Bin
```

An ispec.xml file is created for each deployment folder if you set the *Deploy Winform User Interface* property to True and if you customize the *Final Location* and *Download URI* properties.

The ispec.xml file is created and is available in the Builder Output folder. You can directly use this ispec.xml file as the two properties *DownloadServerURI* and *LocalDownloadDirectory* are already configured.

To locate the ispec.xml file:

1. Locate the Packages directory in the Builder Output folder, in the location <Builder Output Path>\<System Name>\<GUID ID>\Packages.
2. If you have multiple folders in the model, then you will find similar folders inside the Packages directory.
3. Locate the particular Winform folder and open the folder.
4. You will find the ispec.xml file generated for this folder.

The following entries might need to be edited:

1. <system name> should be set to a string with the name of the system. This name appears on the title bar of the Winform window. For example, <system name = "Sample">
2. <startupSystem name> should be set to the same string as <system name>. Note that you can have multiple <system name> sections in the config.xml file. This <startupSystem name> entry specifies which system is started when you first open the Winform Container. For example, <startupSystem name="Sample">
3. <componentName> should be set to the name of the COM Program ID that the system was generated with. Contact your administrator for this value. For example, <componentName>SAMPLE</componentName>.This name is case sensitive and must correspond to the case of the actual name of the COM Prog ID.
4. <runtimeServer> must contain the machine name where the runtime system was deployed and installed. Contact your administrator for this value. Use "localhost" if you generated a test system to your own machine.
5. <downloadServerURI> is where the generated Winform dlls have been copied. For example, <downloadServerURI>http://192.234.333.23/WinFormsDownload/SAMPLE</downloadServerURI>

   or <downloadServerURI>file:///C:\Sample\Release\SAMPLE\Interfaces\WinForms\Bin
6. <GIWCompatibleBehaviour> can be set to true or false. If set to true, then the

behavior of some GUI controls are backwards compatible with a previously used client product called GIW (Graphical Interface Workbench). The specific GIW behavior includes the following:

- Push Buttons: When a push button is pressed, the values associated with all other push buttons on the form is cleared, so that only the value for the pressed push button is sent to the host.
- Radio Buttons: In a radio button group, if no button in the group is set (a default button has not been defined and none of the button values match the value sent from the host) then the first button in the group is set.

Language numbers are added automatically and do not need to be included as part of this entry.

Configuring Winform for ROC

If you want to connect to the Report Output Control System (ROC) from another application using the Roc command, you must first configure the Winforms client to support switching to the ROC system. To do this, add the following XML to the end of the config.xml file:

```
<system name="ROC18">
 <componentName>ROC18</componentName>
 <runtimeServer>localhost</runtimeServer>
 <downloadServerURI>
 file://C:\ROC\Release\ROC18\Interfaces\WinForms\Bin
 </downloadServerURI>
 <localDownloadDirectory>.\</localDownloadDirectory>
 <defaultImageType>.jpg</defaultImageType>
 <defaultImageSubDirectory>images\</defaultImageSubDirectory>
 <defaultListType>.xml</defaultListType>
 <defaultListSubDirectory>lists\</defaultListSubDirectory>
 <disableConsole>false</disableConsole>
 <GIWCompatibleBehaviour>false</GIWCompatibleBehaviour>
 <enableLogging>true</enableLogging>
 <logFile>.\client.log</logFile>
</system>
```

Note: *For 64-bit, you need to modify the <downloadServerURI> entry with the following:*

```
<downloadServerURI>
 file://C:\ROC\Release\ROC18\Interfaces\WinForms\Bin64
</downloadServerURI>
```

Configuring Winform for Cloned Reports

The default Winform configuration file that is used to generate during the build (that is, “ispec.xml” in Core\Bin folder) is based upon the list of reports available in the development model at build time. The creation of report clones using another application (namely, Deployment Package Manager) is a completely separate activity, which is performed in the deployment environment on the target machine. This means that the building of the Winform configuration file does not know anything about which report clones might or might not have been deployed.

However, you can still configure the Winform configuration file to display the cloned reports in Winform in the following way:

Open the Winform configuration file in a text editor and search for the <reports> tag. You can add the following details:

```
<report name=”CLONED_REPORT_NAME”
description=”CLONED_REPORT_DESCRIPTION” />
```

Installing Component Enabler

Before you install the Component Enabler software and any of the generators, you need to install some of the following software depending on your requirements:

- Agile Business Suite Developer and Builder
- Oracle Java Development Kit (JDK) and Java Runtime Environment (JRE) Version 1.6 or later. Java 64-bit is also supported.
- Microsoft .NET Framework 4.7.2 or later
- Microsoft Visual C++ Redistributable for Visual Studio 2017. This requirement is a must for VB.Net Client only.

Note: *Agile Business Suite Component Enabler cannot be installed on a machine on which a previous version of Enterprise Application Component Enabler exists.*

Click **Component Enabler** to begin the installation. The Installation wizard appears and a number of checks are carried out on the system to ensure it has the correct underlying system software to complete a satisfactory installation.

Note: *If two instances of the installation wizard appear, close one instance.*

If the checks are successful, a welcome dialog box is displayed, followed by a license dialog box. Click **Accept** on the license dialog box, if you wish to continue with the installation.

Note: *It is recommended to restart Visual Studio after installing Component Enabler, if Visual Studio was open during the installation of Component Enabler. This must be done, for Visual Studio to recognize the environmental variable settings and to avoid compilation errors during the generation of bundle for presentation client.*

Custom Setup

When you accept the license agreement the Custom Setup dialog box is displayed, which provides the following options:

- Component Enabler for Java
- CE Generate Environment for .NET Framework
  - ASP.NET Web Forms Generator
  - ASP.NET Web Services Generator
  - VB.NET Forms Generator
  - JSP Generator
  - ePortal Generator
- CE Runtime for .NET Framework
- Generator Customization Kit

Component Enabler for Java

If you select **Component Enabler for Java** during your Component Enabler installation, the Component Enabler Runtime and Generate environment for Java are installed as part of the setup program.

Component Enabler Generate environment requires that Java JDK version 1.6 or later be installed on the target machine. When you select Component Enabler and Java JDK version 1.6 or later is not detected, a message box will prompt you to install Java JDK 1.6 or later before selecting this feature.

The Component Enabler installation also installs the Presentation Client software. It is recommended that you must have JDK 1.6 or later to continue the installation.

Note: *The version of JRE must be greater than or equal to JDK. Otherwise, the installer aborts the installation and displays a message.*

CE Generate for .NET Framework

If you select the **CE Generate for .NET Framework** during your Component Enabler installation, the CE Generate for .NET Framework is installed as part of the setup program.

This installs the following files:

- [CERoot]\bin\CEGenerateDotNET.dll
- [CERoot]\bin\CEGeneratorDotNETResources.xml
- [CERoot]\bin\CEGenerateDotNET.xml
- [CERoot]\ReadmeCEGenerateDotNET.htm

The installation registers the CEGenerateDotNET.dll with COM and in the Global Assembly Cache as follows:

```
regasm [CERoot]\CEGenerateDotNET.dll
/tlb:[CERoot]\CEGenerateDotNET.tlb
gacutil –i [CERoot]\CEGenerateDotNET.dll
```

The CEGenerateDotNET.dll can be unregistered as follows:

```
gacutil /u CEGenerateDotNET,PublicKeyToken=d75f28b512e9147c
regasm [CERoot]\CEGenerateDotNET.dll /unregister
```

This feature requires that .NET Framework 4.7.2 be installed on the target machine. When you select this feature and .NET Framework 4.7.2 is not detected, a message box will prompt you to install .NET Framework 4.7.2 before selecting this feature.

ASP.NET Web Forms Generator

If you select the **ASP.NET Web Forms Generator** during your Component Enabler installation, the ASP.NET Web Forms Generator is installed as part of the setup program.

When you select this feature and you have not selected either CE Runtime for .NET Framework or CE Generate for .NET Framework, a message box will prompt you to install one of those feature options.

The ASP.NET Generator in the AB Suite 7.0 Release includes support for AJAX technology.

In order to install and run the generator you need to have the following additional system software installed above the base Component Enabler software requirements.

- Microsoft .NET Framework 4.7.2 or later
- Microsoft Visual Studio (optional).

  This is only required on the generation workstation if you wish to modify the generated project file in order to perform customization prior to compiling the files as an ASP.NET Web Forms application
- Microsoft Internet Information Services 10.0 or later (optional).

  This is only required on the generation workstation if you wish to deploy and test the ASP.NET Web Forms Application locally.

The Web Server

- Microsoft .NET Framework 4.7.2 or later
- Microsoft Internet Information Services 10.0 or later

The Application Server

TCP/IP capability is required on the Enterprise Application System with the Remote Access server software and the web server.

Installation Structure

The installation creates a new subdirectory called ASP.NET Generator in the installed Component Enabler Directory (for example, ..\ASP.NET Generator).

The C# version of the ASP.NET Web Forms Generator is a dll called GenerateFormASPdotNET.dll, which is copied into the Component Enabler “Bin” directory for use by the CE .NET Generate environment.

The ASP.NET Web Forms Generator installation directory includes the following sub directories:

- Bin – Contains two dll's called UniCombo.dll and UniMenu.dll. They are used at runtime to provide support for combo-boxes and a right-click context menu in the ASP.NET Web Forms.
- Common – Contains infrastructure files that are common to the entire application.
- Images – Contains a default image called blank.gif, which is used when the requested image file is not found at runtime.
- Lang – Contains infrastructure files that can be customized for each language of an application.
- Utilities\Setup – Contains sample scripts that can be used to compile the generated files and establish the Virtual directory for the ASP.NET application. The SetupASPNet.vbs script creates a specified Virtual directory, a physical directory and copy the required files across from the installed ASP.NET Web Forms Generator directories into the correct locations.

Configuration

Specify <Install Directory>\Bin\GenerateFormASPdotNET.dll as the User Defined View Generator in the CE Folder properties.

ASP.NET Web Services Generator

If you select the **ASP.NET Web Services Generator** during your Component Enabler installation, the ASP.NET Web Services Generator is installed as part of the setup program.

When you select this feature and you have not selected either CE Runtime for .NET Framework or CE Generate for .NET Framework, a message box will prompt you to install one of those feature options.

In order to install and run the generator, you need to have the following additional system software installed above the base Component Enabler software requirements.

The Generation Workstation

- Microsoft .NET Framework 4.7.2 or later
- Microsoft Visual Studio (optional)

  This is only required on the generation workstation if you wish to modify the generated project file in order to perform customization prior to compiling the files as a Web Services.
- Microsoft Internet Information Services 10.0 or later (optional)

  This is only required on the generation workstation if you wish to deploy and test the Web Services locally.

The Web Server

- Microsoft .NET Framework 4.7.2 or later
- Microsoft Internet Information Services 10.0 or later

The Application Server

TCP/IP capability is required on the System with the Remote Access server software, and the web server.

Installation Structure

The installation creates a new subdirectory called Web Services .NET Generator in the installed Component Enabler Directory (for example, ..\Web Services .NET Generator.

The C# version of the Web Services .NET Generator is a dll called GenerateWSdotNET.dll. This dll file is copied into the Component Enabler Bin directory for use by the CE .NET Generate environment.

The Web Services .NET Generator installation directory includes the following sub directories:

- common\views – contains infrastructure files such as error checking files, a configuration XML file and a compiler batch file.
- utilities\BundleViewSetp – contains Visual Basic script files.
- utilities\discoveryTool – contains a Web Service Discovery tool for testing generated Web Services.

Configuration

Specify <Install Directory>\Bin\GenerateWSdotNET.dll as the User Defined View Generator in the CE Folder properties.

VB.NET Forms Generator

If you select the **VB.NET Forms Generator** during your Component Enabler installation, the VB.NET Forms Generator is installed as part of the setup program.

When you select this feature and you have not selected CE Runtime for .NET Framework and CE Generate for .NET Framework, a message box will prompt you to install one of those feature options.

JSP Generator

If you select JSP Generator during your Component Enabler installation, the JSP Generator is installed as part of the setup program. When you select this feature, the CE Generate for .NET Framework is installed.

In order to install and run the JSP Generator you must have the following additional system software installed above the base Component Enabler software requirements.

- Oracle JRE and JDK – 1.6 (jdk-7u51-windows-i586.exe) or 1.7 (jdk-7u3-windows-i586.exe)

  Note: *JDK is required for Presentation Client and JSP Client generation.*

- Java based IDE. For example, Eclipse

This is only required on the generation workstation if you wish to modify the generated jsp files in order to perform customization prior to compiling the files as a JSP Web application.

- Apache Tomcat 6.0 or 7.0 (apache-tomcat-6.0.26-windows-x86)

This is required if you wish to run the JSP Web application.

Installation Structure

The installation creates a new subdirectory, JSP Generator in the installed Component Enabler Directory (for example, ..\JSP Generator).

The JSP Client Generator is a .NET assembly called GenerateFormJSP.dll, which is copied into the Component Enabler Bin directory for use by the CE .NET Generate environment.

The JSP Client Generator installation directory includes the following sub directories:

- Common – Contains infrastructure files that are common to the entire JSP application.
- Lang – Contains infrastructure files that can be customized for each language of a JSP application.
- Utilities\Setup – Contains scripts that establish the virtual directory for the JSP application. The sample script, SetupJSP.vbs is a wizard that guides the user through the steps for setting up the folder structure for the Web Application, copies all necessary infrastructure files into the Tomcat_home/webapps directory. The ce.properties file, which is located at, TOMCAT_HOME\webapps\<application_name>\WEB_INF\classes is updated with values for the following properties.

  - Application Name
  - Bundle Name
  - Package Prefix

  You must update the following values in the ce.properties file manually.

  - Username
  - Password
  - View name
  - Host name
  - Host port

Configuration

To use the JSP Client Generator, you must specify GenerateFormJSP.dll as the User Defined View Generator in the CE Bundle Folder properties of the System Modeler or EAE Developer.

CE Runtime for .NET Framework

If you select the **CE Runtime for .NET Framework** during your Component Enabler installation, the CE Runtime for .NET Framework is installed as part of the setup program.

This feature requires that .NET Framework 4.7.2 be installed on the target machine. When you select this feature and .NET Framework 4.7.2 is not detected, a message box will prompt you to install .NET Framework 4.7.2 before selecting this feature.

Generator Customization Kit

If you select the **Generator Customization Kit** during your Component Enabler installation, you are prompted for a valid password. The password is the software key for the Client Generator Customization Kit, provided in the key document that accompanies the Component Enabler Software. Once you supply this password, the Generator Customization Kit is installed as part of the setup program. It is installed within the Component Enabler directory structure in its own folder.

Completing the installation

When you have selected the components that you want to install, click **Next** to display the Ready to Install the Program Screen and click **Install** to proceed with the installation, otherwise click **Back** to make changes.

After the installation has finished, the Installation Complete Screen is displayed. Click **Finish** to complete the installation.

Oracle JRE Installation and Configuration

The Oracle JRE v1.6 or later is used in Builder to generate Component Enabler files. It can also be used with clients that rely on the COM/Java bridging support which the Microsoft JVM has previously provided (for example, VB Clients, Active Server Pages, etc.). This functionality is now being supported by the ActiveX Bridge feature that is available in the Oracle JRE v1.6 or later. The following information describes the procedure required to setup the Component Enabler Development and Runtime environments for use with the Oracle JRE ActiveX bridge functionality.

Development Environment Generate Setup (Oracle JRE - ActiveX Bridge)

To configure your Development environment for use with the Oracle JRE, perform the following:

1. Download the Oracle Java from the Oracle Java Web Site at https://www.oracle.com/java/technologies/javase-java-archive-javase6-downloads.html.
2. Install Java, that is, both JDK and JRE.
3. If you have not already done so, install Component Enabler from the installer.
4. Depending on your environment configuration, you might need to adjust the necessary levels of security for running the Component Enabler Generator functionality through the Java Plugin. The Java policy file is called "java.policy" "default.policy" and is located in the <JRE_HOME>\lib\security directory.

   For example:

   ```
   C:\Program Files\Java\j2re1.6.0\lib\security\java.policy
   ```

   In order to provide the Component Enabler generation environment with access to the required machine resources through the Java Plug-in, the following setting is automatically included by the Component Enabler Installation program. In most cases, you will not need to adjust it. However, if it is removed or the policy file is replaced at any stage, you might see security violation errors appearing in the Java Console, and the generate is not completed successfully. If this occurs, you must add the following permission manually.

   ```
   grant codeBase "file:C:\\NGEN_CE\\lib\\*" {
    permission java.security.AllPermission;};
   ```

   While this requires less effort than setting individual permissions, to achieve the necessary results, it does increase the security risk on the machine. It means that a Java application in that codeBase specification will have unrestricted access to the machine resources. When dealing with Unisys supplied components this should not be a problem. However, you might wish to incorporate more stringent security than the above permission provides. If so, you can remove the AllPermissions setting and ensure that the following are the minimum permissions that are set in order for the application to work correctly.

   Note: *In case of Java 32-bit, the Java.policy file is updated automatically during the installation of the Component Enabler. If you have Java 64-bit installed, then perform the instructions as mentioned above.*

   - To create the Generate.Log file in the C:\Temp directory, add the following permission

     ```
     permission java.io.FilePermission
      "c:\\temp\\GENERATE.LOG","write";
     ```

   - To create the output files from the generate (for example, IspecModel classes, ASP Forms, VB Forms) permissions are set by default for the directory "C:\NGEN_CE\Classes". This directory must match the directory specified in Developer for the output directory of the Component Enabler bundle. For example, if you have specified C:\NGEN_CE\Classes in the Application Bundle details, then the file permission should be:

     ```
     permission java.io.FilePermission
      "C:\\NGEN_CE\\classes\\-","read,write";
     ```

5. Before you can generate Component Enabler files from Builder, the Java Plug-In Runtime Parameters need to include the CLASSPATH for the JAR files required by

the generate process. Add the classpath settings as a Java Runtime Parameter in the Advanced Tab of the Java Plug-In Control Panel. This allows the ActiveX bridge software to find the Jar files required for the Generate.

For example:

```
–cpc:\NGEN_CE\classes;c:\NGEN_CE\lib\generate.jar;
c:\NGEN_CE\lib\lincapplet.jar;c:\NGEN_CE\lib\lincviewer.jar;
c:\NGEN_CE\lib\ASPGenerator.jar;c:\NGEN_CE\lib\WSGenerator.jar;
c:\NGEN_CE\lib\VBGenerator.jar;
```

Note: *If you have not installed all the optional generators, ASP, WS, or VB it is recommended to still add these paths on completion of the initial installation to avoid possible future errors if the generators are installed at a later date.*

WorkStation Client Setup (Oracle JRE with ActiveX Bridge)

To configure your workstation client runtime environment to use the Oracle ActiveX bridge instead of the Microsoft JVM COM-Java support, perform the following:

1. In order to run the generated VB client or any other COM-based client that you have developed, you need to register the LINCEnvironment class.

   Unlike previous releases, the ActiveX bridge binaries for custom Java generators is not copied to the target machine during the installation of Component Enabler. Instead these files are placed inside a folder, **axbridge**, in the Component Enabler folder of the Developer installer.

   The installer of Component Enabler gives priority to Java 64-bit. If the machine has both Java 32-bit and 64-bit installed, Component Enabler gets bound to Java 64-bit.

2. In order to deploy the Component Enabler client application to another machine, copy the axbridge folder and its contents to the <JRE_HOME> in the target machine.

   This step also copies the LINCApplet.Jar file that contains the LINCEnvironment class into the corresponding “lib” directory.

   For example:

   ```
   <JRE_HOME>\axbridge\lib\LincApplet.jar
   ```

   Notes:

   - *To determine whether you have Java 32-bit or 64-bit installed. You can check the registry key as follows:*

     For example:

     If you have Java 32-bit installed in 32-bit environment:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment
     ```

     and

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Development Kit
     ```

     If you have Java 32-bit installed in 64-bit environment:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\
     JavaSoft\Java Runtime Environment
     ```

and

```
HKEY_LOCAL_MACHINE\SOFTWARE\\Wow6432Node\
JavaSoft\Java Development Kit
```

If you have Java 64-bit installed in 64-bit environment:

```
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment
```

and

```
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Development Kit
```

- *Determine the JRE home.*

  For example:

  For Java 1.6 32-bit in a 64-bit environment:

  ```
  C:\Program Files (x86)\Java\jre6
  ```

  For Java 1.8 64-bit in a 64-bit environment:

  ```
  C:\Program Files\Java\JRE1.8.0_92
  ```

3. Once the dll is in place on the client machine, run the command prompt as Administrator, execute the regsvr32 command to register the dll.

   For example:

   In a 32-bit machine:

   ```
   C:\Windows\System32\regsvr32.exe /s
   "<JRE_HOME>\axbridge\bin\LINCEnvironment.dll"
   ```

   and

   ```
   C:\Windows\System32\regsvr32.exe /s
   "<JRE_HOME>\axbridge\bin\GenerateProxyLDA.dll"
   ```

   In a 64-bit machine:

   ```
   C:\Windows\SysWOW64\regsvr32.exe /s
   "<JRE_HOME>\axbridge\bin\LINCEnvironment.dll"
   ```

   and

   ```
   C:\Windows\SysWOW64\regsvr32.exe /s
   "<JRE_HOME>\axbridge\bin\GenerateProxyLDA.dll"
   ```

4. In your application, specify the class to be used when creating the LINCEnvironment object. For a generated VB application, modify the Class_Initialize() subroutine of the EAEEnvironment.cls module, in order to select the appropriate method for creating the LINCEnvironment object. Use the following line of code for the Oracle ActiveX bridge environment:

   ```
   Set mobjLinc = CreateObject("LINCEnvironment.Bean.1")
   ’ Oracle JVM with ActiveX bridge
   ```

   Ensure the alternative line of code for using the Microsoft JVM is commented out.

5. Add the classpath settings as a Java Runtime Parameter in the Advanced Tab of the Java Plug-In Control Panel. This allows the ActiveX bridge software to find the Component Enabler IspecModel classes that have been deployed to the workstation.

For example:

```
-cp c:\NGEN_CE\classes;
```

6. Update the Java policy file. Depending on your environment configuration, you might need to adjust the necessary levels of security for running the VB Client using the ActiveX bridge through the Java Plugin. The Java policy file is called "java.policy""default.policy" and is located in the <JRE_HOME>\lib\security directory.

   For example:

   ```
   C:\Program Files\Java\j2re1.6.0\lib\security\java.policy
   ```

7. The following settings might need to be added to provide the Component Enabler Runtime environment with access to the required machine resources. If they are omitted, you might see security violation errors appearing in the Java Console, and the client application will not run successfully.

   - Socket Permission – This grants access to the machine that hosts your Agile Business Suite Runtime application:

     For example:

     ```
      permission java.net.SocketPermission "HostComputer",
     "connect,resolve"; // Where Host Computer
     is the computer name on the Domain or the IP Address.
     ```

   - Runtime Permission – The following two entries might be necessary when running the generated VB client application

     ```
     permission java.lang.RuntimePermission "modifyThreadGroup";
     permission java.lang.RuntimePermission "modifyThread";
     ```

   - File Permission – If you have set up the Client application to perform logging using the Component Enabler Log object, you need to specify a File Permission giving the name and location of the log file.

     For example:

     ```
     permission java.io.FilePermission
     "c:\\temp\\VBClient.log","write";
     ```

     Note: *An alternative to setting individual permissions for either the development or runtime environment, would be to set the AllPermission permission on the Component Enabler codeBase directory.*

     For example:

     ```
     grant codeBase "file:C:\\NGEN_CE\\lib\\*" {
     permission java.security.AllPermission;
     };
     ```

     While this requires less effort to achieve the necessary results, it does increase the security risk on the machine. It means that a Java application in that codeBase specification will have unrestricted access to the machine resources. When dealing with Unisys supplied components, this should not be a problem.

Installing the Presentation Client

The Presentation Client can be installed independently of the Component Enabler Development environment. Select **Presentation Client** on the main setup window to install the Presentation Client as a standalone client on a user workstation.

Notes:

- *If two instances of the installation wizard appear, close one instance.*
- *The Presentation Client is installed by default with the Component Enabler Development environment. A development workstation does not need to re-install the Presentation Client using this option.*

The Presentation Client can also be configured on a Web server to run as an applet within a browser client. Refer to **Unresolved xref: linkend =** **.**

Requirements

For both standalone client and browser client modes, you require a network machine with TCP/IP services installed.

Standalone Client

The following operating systems have been tested and are supported for use with the Presentation Client:

- Windows 10 Enterprise (x64), Professional (x64)
- Windows Server 2019 Standard, Datacenter
- Windows Server 2016 Standard, Datacenter
- Apple Macintosh OS X

The Java 2 Runtime Environment (JRE) Version 1.6 or later is required on the client workstation.

Browser Client

The following table shows some additional requirements for the Presentation Client running in a browser:

Requirement	Description
Browser	Microsoft Internet Explorer 11.0 or later. All other browsers including mobile browsers. ***Note:*** • *If using Macintosh, you require Safari 3.1.2 or later.* • *Browser-based Presentation Client runs in the browser as a Java Applet. Java Applet support has been officially terminated for Chrome (45 onwards), Edge, and most of the other modern browsers through the end of support of NPAPI on those browsers. Therefore, browser-based Presentation Client will only run on Internet Explorer 11 until support for Java applets or Internet Explorer is terminated.* *It is recommended that you use the ASP.NET and JSP clients as browser-based Component Enabler client alternatives, or consider distributing the desktop-based Presentation Client, which continues to be supported.*
Java Plug-in	Oracle Java Plug-in Version 1.6 or later.

Setup

Depending on the mode of operation, your environment can be set up in different ways and installation files might be allocated to different locations.

The installation files are described in the following tables:

Standalone client specific

File	Description
LincViewer.jar	Contains the class files that are required to run the Presentation Client as an application.

Browser client specific

File	Description
LincViewer.jar	Contains the class files that are required to run the Presentation Client as an application.
Home_page.html	A sample home page to start the Presentation Client as an applet in a browser.
TCP/IP redirector	Utility program to allow the connection to be routed through the Web server back to the host application.

Common files

File	Description
Configuration file	Contains the configuration parameters for connecting to host applications.
ViewerResources.properties	Contains localization and internationalization strings.
Class files	The generated class files for the Enterprise Application Environment application.
Images and Lists	Any images or list box data files required by the graphical screens.
Jh.jar	Support library for Java Help.
ViewerHelp.jar	Contains the online help for the Presentation Client.
XmlParserAPIs.jar XercesImpl.jar	Support library for reading XML formatted configuration files.

Standalone Installation for Windows Operating Systems

Selecting this installation option installs only those files required to run the Presentation Client as a standalone application on a Windows workstation.

1. On the main Client Environment installation screen, select **Presentation Client**.
2. Specify the installation directory. The default directory is displayed, but you might select another location.
3. A default configuration file, config.xml, is copied to the installation directory. The default configuration file initially has no entries, as configuration information is site-specific. However, the administrator can update the file using the Configuration Assistant (or manually using a text editor).

   The updated file can be included as part of a customized version of the Presentation Client installation image. When the customized Presentation Client installation package is exercised, the updated configuration file is copied to the Presentation Client installation directory. Refer to Customizing the Presentation Client Installation for more information.

A shortcut is added to the Start screen, All apps, Agile Business Suite 7.0, Presentation Client. The shortcut references the default configuration file, config.xml.

Standalone Installation for non-Windows Operating Systems

The installation of the Presentation Client on non-Windows platforms is a manual process:

1. Set up the Presentation Client directory on the workstation; for example, C:\NGEN_CE\Presentation Client.
2. Copy the Presentation Client jar files to the directory. Ensure the following files are copied:
   - jh.jar
   - ViewerHelp.jar
   - LINCViewer.jar
   - xmlParserAPIs.jar
   - xercesImpl.jar
3. Set up a directory which class files can either be copied to, or downloaded from a remote location; for example, C:\CE\classes.
4. Copy the configuration file to the Presentation Client directory, or another accessible location. Refer to Using the Configuration Assistant in the *Agile Business Suite Component Enabler Guide* for more information on creating a configuration file.
5. Ensure the following files and directories are included in the classpath:
   - Viewer.jar file.
   - Location of the generated form class files. If these files are not located within the Presentation Client directory, the download destination option must be specified in the configuration file.
6. Ensure the Java Runtime Environment (version 1.6 or later) is installed on the workstation.

To start the Presentation Client, run the Java interpreter from the command line using the following syntax:

```
javaw com.unisys.jellybeans.views.LINCViewer <command line options>
```

The following example starts the Presentation Client as an application accessing the system sample, as defined in the configuration file *config.xml*.

```
javaw com.unisys.jellybeans.views.LINCViewer -config=config.xml -system=sample
```

If applicable, you can create a desktop icon or menu item to initiate the Presentation Client.

Uninstalling the Presentation Client

Uninstalling the Presentation Client on non-Windows platforms is a manual process. It is a matter of reversing the installation instructions and deleting the relevant files.

Using the Redirector

If an applet needs to make a socket connection to a socket other than the one from which it was originally loaded, the connection to the Remote Access server has to pass through a redirector program on the Web server. This occurs if the system and the Web server supplying the client components are running on different systems.

A redirector program for the Windows 10 environment is supplied with AB Suite 7.0, as CE\ReDIR\tcpredir.exe.

There are two commands to use with the redirector:

- **`tcpredir –install`**

  installs the redirector.

  ```
  tcpredir –install
   <1st lport#>:<1st machine name>:<1st rport#>
   <2nd lport#>:<2nd machine name>:<2nd rport#>
  ```

  where:

  – “lport#” is the port number to listen on

  – “machine name” is the name of the machine to redirect to

  – “rport#” is the port number to redirect to

  This allows the Web server to connect to multiple systems. After installing the redirector, you must start it before can be used.

  To start the redirector, go to **Control Panel**, **Services** on your Web server. Select **TCP Redirector**, and then click **Start**. To stop the redirector, go to **Control Panel**, **Services**, select **TCP Redirector**, then click **Stop**.

- **`tcpredir –remove`**

  removes the redirector.

Using Component Enabler with Browsers

Component Enabler has been qualified with the Microsoft Internet Explorer Web browser. You can download Microsoft Internet Explorer from:

http://www.microsoft.com/ie/

Using Component Enabler with COM Based Applications

In order to access COM based applications using Component Enabler, you have a couple of options: (1) Use the Oracle Java Plugin with the ActiveX Bridge support for the Java/COM interface. (2) Use the CEWindowsAPIJavaStyle interface in the .NET based Component Enabler Runtime. Refer to the *Agile Business Suite Component Enabler User Guide* for more information about interfacing to COM based applications.

Customizing the Presentation Client Installation

The Presentation Client installation software includes several configuration options that allow you to prepare a customized version of the installation package. The administrator can make a copy of the Presentation Client installation directory from the Client Environment folder, present within the CD Developer folder, and then make modifications in certain areas to develop a Presentation Client runtime installation package that meets site-specific requirements. The areas that can be customized are described below.

Default Configuration File

A skeleton configuration file called config.xml is provided in the installation directory for the Presentation Client. This configuration file can be overwritten by the administrator with a site-specific configuration file prepared with the Configuration Assistant. A copy of the Presentation Client installation directory can include the new configuration file. This can then be used for installation on user workstations at the customer site.

Icons

If the configuration file refers to specific icons that the Presentation Client requires at runtime, these icons can be copied to the...\Icons directory of the installation package. The contents of the icons directory is copied to the installation directory of the user's workstation.

Application Classes

The generated application classes for an Enterprise Application Environment system can also be bundled with the Presentation Client installation. Copy the classes to the...\Classes directory of the installation package.

During installation, the directories and files within the Classes directory of the installation package is copied to a Classes directory beneath the installation directory on the user's workstation.

The Java class files must be assembled within the required Java package structure, and this is maintained during installation.

For example, if you have generated a system called "sample" with a package prefix of "com.unisys" and a bundle name of "all", the structure beneath the ...\Classes directory should contain the following directories and associated contents:

```
Com\unisys\sample\all\ispecs (Data classes)
Com\unisys\sample\all\views\lang1 (Presentation classes)
```

This level of customization allows workstations to be initially set up with all the required runtime components to achieve a connection with the Enterprise Application Environment system using the Presentation Client. Subsequent updates can then be downloaded as necessary from a Web server.

This type of installation customization is suited to users that want to use software distribution mechanisms to deploy the Presentation Client and associated runtime components, to many user workstations. In conjunction with the silent mode operation (refer to Presentation Client Silent Installation), this offers a convenient mechanism for installing the Presentation Client software, and also configuring it with the required site-specific components and configuration options.

Presentation Client Silent Installation

Automated electronic software distribution (silent install) enables the installation of Presentation Client as a stand-alone application across a number of Windows operating system workstations, thus reducing administration time and ensuring consistent environments. Silent installation can be used in conjunction with System Management Services to automatically install Presentation Client from network servers on a large number of workstations.

Requirements

Before running the silent installation, ensure the JRE is installed on the target workstations, as it is not included with the silent installation. You can perform a silent installation of the Java Runtime Environment by performing the instructions in https://docs.oracle.com/javase/8/docs/technotes/guides/install/windows_installer_options.html.

Performing a Silent Installation

A response file is required in order to run a silent installation. The response file can either be created automatically or manually. The following procedure for performing a silent install includes the automatic creation of the response file.

Step 1: Automatically creating a response file

1. From the command prompt change the location to the directory containing the Setup.exe file.
2. Run the installation including the additional flags.

   ```
   -a -r /f1<path><filename.iss>
   ```

   where:

Flag	Description
-a	Signals that additional parameters are to be passed to the executable file.
-r	Sets the installation in record mode.
-f1	Specifies the location and name of the response file to be created, where *<path>* is the location and *<filename.iss>* is the file name. If this switch is omitted, the default file setup.iss is created in the Windows directory.

   For example,

   ```
   Setup.exe -a -r /f1C:\CEInstall\CEsetup.iss
   ```

   Note: *There is no space between /f1 and <path>.*

3. Proceed through the installation process and select the options you want to use in the silent installation.

When the installation is complete the response file is created in the specified directory and contains information similar to the following example:

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-DlgOrder]
Dlg0={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdWelcome-0
Count=7
Dlg1={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdLicense-0
Dlg2={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-AskText-0
Dlg3={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdAskDestPath-0
Dlg4={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdSelectFolder-0
Dlg5={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdStartCopy-0
Dlg6={2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdFinish-0
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdWelcome-0]
Result=1
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdLicense-0]
Result=1
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-AskText-0]
szText=11779900
Result=1
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdAskDestPath-0]
szDir=C:\Alinc
Result=1
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdSelectFolder-0]
szFolder=Enterprise Application Component Enabler
Result=1
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdStartCopy-0]
Result=1
[{2EFFFB81-3AAF-493B-B3A9-E52542AA555F}-SdFinish-0]
Result=1
bOpt1=1
bOpt2=0
```

Step 2: Running the silent install

No messages are displayed when running a silent installation. You can create a log file in which all the installation information is recorded.

1. Uninstall any previously installed versions of Presentation Client.
2. To run the installation in silent mode you must first record your actions, and secondly you must run in the silent mode using the recorded script file.

   To record:

   ```
   -r /f1<path><filename.iss>
   ```

   For example,

   ```
   Setup.exe -r /f1"C:\setup.iss"
   ```

   To run in silent mode:

   ```
   Setup.exe -s /f1"C:\setup.iss"
   ```

Flag	Description
-s	Sets the installation into silent mode.
f1	Specifies the location and name of the response file, where *<path>* is the location and *<filename.iss>* is the file name.
-r	To record the installation to the script file so the silent installation can use it.

Step 3: Checking the log file for errors

To verify the success of the silent install, check the ResultCode value in the [ResponseResult] section of the log file. This value should be zero.

One of the following values is returned as the ReslultCode:

Value	Description
0	Successful installation
-1	General error
-2	Invalid mode
-3	Required data not found
-4	Insufficient memory available
-5	File does not exist
-6	Cannot write to response file
-7	Cannot write to log file
-8	Invalid path to the InstallShield Silent response file
-9	Not a valid list type (string or number)
-10	Data type invalid
-11	Unknown error during setup
-12	Dialog boxes are out of order
-51	Cannot create the specified folder
-52	Cannot access the specified file or folder
-53	Invalid option selected

Manually Creating a Response File

Rather than using the automatic process described in the preceding procedure, you can create a response file manually.

The response file has an .iss extension and is similar to an .ini file. The sections of an InstallShield response file must be in the following order:

1. **Silent Header**

   All response files begin with a silent header. The silent header enables InstallShield to identify the file as a valid response file.

   The silent header section must contain the following parameters and values:

   ```
    [InstallShield Silent]
   Version=v6.00.000
   File=Response File
   ```

   Version indicates the version of InstallShield, it is not necessary to specify the specific release level. Use v6.00.000 in all response files. Future versions of Installshield is able to read this version of the response file.

2. **Application Header**

   This is the second section in the response file. It allows developers of the installation setup to identify the setup for which the response file was created, as this is often difficult to determine by looking at the other response file data. It is not used by the setup script or the Setup.exe file.

   The application header section contains the following parameters and values:

   ```
    [Application}
   Name=<ProductKey from InstallationInfo>
   Version=<VersionKey from InstallationInfo>
   Company=<CompanyKey from InstallationInfo>
   ```

   These values are derived from the values written to the registry in the call to the Installation Info function in your setup script.

3. **Dialog Sequence**

   This is the third section in the response file. It lists all the dialog boxes needed during the installation, in the order in which they appear. This section is given the heading:

   ```
   [<Product_GUID>-DlgOrder]
   ```

   The dialog box parameters are formatted as follows:

   ```
   Dlg<#>=<PRODUCT_GUID>=<DialogIdentifier>-Dlg-<#>
   ```

   The dialog box numbering sequence begins at zero, meaning the first parameter entry is Dlg0. Each subsequent dialog box number increments by one.

   The section is ended with the Count parameter, the value of which equals the number of dialog boxes listed. Because the dialog box sequence begins with zero, the Count value is always one greater than the highest dialog box number.

   For example,

   ```
   [{23EAFFCA-361D-11D3-8B0F-00105A9846E9}-DlgOrder]
   Dlg0={23EAFFCA-361D-11D3-8B0F-00105A9846E9}-Welcome-0
   Dlg1={23EAFFCA-361D-11D3-8B0F-00105A9846E9}-AskOptions-1
   Count=2
   ```

4. **Dialog Box Data**

The values entered in each dialog box are captured in the response file. Each dialog box listed in the dialog sequence section has its own section.

```
[<PRODUCT_GUID>-<DialogIdentifier>] Result=<value>
Keyname1=<value>
Keyname2=<value>
```

- **`[<PRODUCT_GUID>-<DialogIdentifier>]`**

  identifies the specific dialog box, where <DialogIdentifier> is the value entered for the dialog box in the dialog sequence section.

- Data entered in a dialog box is recorded in the form **Keyname=<value>**. All dialog boxes return the keyname **Result**, which indicates the button pressed to exit the dialog box. The standard values for **Result** are 12 for the Back button, and 1 for Next or OK.

  The keynames for the InstallShield dialog boxes are listed in the following table:

Dialog Box	Keynames	Description
SdWelcome-<#>	Result	1 = Next
SdLicense-<#>	Result	1 = Yes is selected
AskText-<#>	szText	The text from the edit field
	Result	1 = Next
SdAskDestPath-<#>	szDir	The path specified in the edit field
	Result	1 = Next
SdSelectFolder-<#>	szFolder	The folder specified in the edit field
	Result	1 = Next
SdStartCopy-<#>	Result	1 = Next
SdFinish-<#>	bOpt	1 = “Yes, I want to view the README file” is selected
		0 = “Yes, I want to view the README file” is not selected
	bOpt2	bOpt2 is always 0

Installing Business Integrator

Select **Business Integrator** during the Client Environment installation to start the Business Integrator installation. The Installation wizard appears.

Note: *If two instances of the installation wizard appear, close one instance.*

Refer to the *Agile Business Suite Getting Started with Business Integrator Guide (38265898)* in the Documentation folder, present within the CD Developer folder.

External Components

To run the Business Integrator External Components environment, the following software is required:

- Microsoft Management Console (MMC) 1.2 or later
- Microsoft XML Parser (MSXML) 4.0 and 6.0
- Microsoft Visual C++ 2010 Redistributable Package(x86) might need to be installed manually. Refer to the *Agile Business Suite Business Integrator Getting Started Guide* for more information.

Installing Client Framework

You can install the Client Framework standalone software from the installer as a standalone component on the end-user workstation.

The Client Framework standalone component includes a complete WPF Container application that hosts the Views assembly and displays a view that corresponds to a particular ispec. It also includes the AB Suite Client Framework MVC Scaffolder and the NuGet Packet Manager for Visual Studio 2017.

To install the Client Framework standalone software, perform the following:

1. Click **Client Framework (32-bit)** or **Client Framework (64-bit)** on the Client Environment interface. The Installation wizard appears and a number of checks are carried out on the system to ensure it has the correct underlying system software to complete a satisfactory installation.

   Notes:

   - *If two instances of the installation wizard appear, close one instance.*
   - *If the Client Framework software is already installed on your machine as a separate instance, the Program Maintenance dialog box appears; you can choose to repair or remove the Client Framework software.*

2. If the checks are successful, a welcome dialog box appears, followed by a license dialog box. To accept the conditions and continue with the installation, click **I accept the terms in the license agreement**; if not, click**I do not accept the terms in the license agreement**.

   Accepting the license agreement allows you to select the target drive and directory for the installation, if you do not want to accept the default installation location.

3. Click **Next** to proceed with the installation.

   You can click **Back** to make changes, if any.

   At the completion of the installation, the Installation Shield Wizard Completed dialog box appears. This screen allows you to view the readme file and the Windows Installer log file. If you want to view the readme file or the Windows Installer log file, select the respective check box.

4. Click **Finish** to complete the installation.

Configuring WPF Client Container

Before running applications, you must edit the “<Client Technology Folder Name>_Config.rtxml” configuration file. For example, if the Client technology folder in System Modeler has the name “WPFClient”, the configuration file should be “WPFClient_Config.rtxml”. This file contains configuration information to enable the WPF client to find and connect to the application component. This file is automatically created during the generation of the system. The administrator might have already modified this configuration file in the installation package. Check with your administrator before proceeding to modify the file.

A default copy of the configuration file is located at <System Modeler project folder>\Access Layer API Deploy.

The following entries of the configuration file might need to be edited:

- <system name> should be set to a string with the name of the system. This name appears on the title bar of the WPF client application window; for example, <system name = “Sample”>
- <startupSystem name> should be set to the same string as <system name>. Note that you can have multiple <system name> sections in the configuration file. This <startupSystem name> entry specifies which system is started when you first open the WPF Client; for example, <startupSystem name=”Sample”>
- <componentName> should be set to the name of the COM Program ID that the system was generated with for example, <componentName>SAMPLE</componentName>. Contact your administrator for this value. This name is case-sensitive and must correspond to the case of the actual name of the COM Prog ID.
- <runtimeServer> must contain the machine name where the runtime system was deployed and installed. Contact your administrator for this value. Use “localhost” if you generated a test system to your own machine.
- <downloadServerURI> is a location where the required WPF Client assemblies are retrieved from. This can be a file share on the local or remote machine; for example, <downloadServerURI>file://C:\Users\<User Name>\Documents\Visual Studio 2017\Projects\ForwardModel\Access Layer API Deploy. It can also be an FTP or HTTP site from where you can download the assemblies.

To run the WPF Client Container, setup a shortcut that allows you to specify the name and location of the Configuration file as a parameter; for example, “<WPFClient Installation Path>\WpfClient.exe” “C:\Users\<UserName>\Documents\Visual Studio 2017\Projects\<Technology Folder>\Access Layer API Deploy\WpfClient_Config.rtxml”.

Installing Windows TLS Certificate

For Windows clients, while using Secure RATL, OS2200 Secure FTP, MCP Secure FTP, the appropriate TLS certificates must be installed in the Microsoft Management Console (MMC) in the host where application bundle is available. The chain of certificates required for the TLS connection must be installed in the client machine.

Perform the following steps to install the certificate:

1. Click **Start**, point to **All apps**, expand **Windows System**, and then click **Run**. Enter certlm.msc in the **Run** window. Alternatively, enter certlm.msc in the search box, and then press the **Enter** key.
2. To import the certificate into Trusted Root Certificate Authorities in Certificates, expand **Trusted Root Certificate Authorities** and select **Certificates**.
3. Right-click **Certificates**, point to **All Tasks** , and then click **Import**.
4. Click **Next** in the **Certificate Import Wizard**.
5. Browse to the path where the certificate that you want to install is located, and then click **Next**.
6. Click **Finish**.

   A pop up is displayed to indicate that the import is successful.

   Certificates are installed successfully and can be viewed under the **Trusted Root Certificate Authorities** in **Certificates**.

Note: *When configuring the client for Secure RATL, the HostURI should be entered in the format"x-<protocol>:<hostname>:<port>", where protocol is ratltls instead of ratl , the hostname is the name of the server machine where runtime application is running and the port number is the port on which RATL service is running in server machine.*

For example,

```
  "<add key="HostURI" value="x-ratltls:localhost:2448"/>"
```

To enable Secure FTP for AB Suite 7.0 MCP deployment, the Registry setting SecureFTP must be created under

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\UNISYS\System Modeler\Features\Builder
```

Change, Repair, or Uninstall Agile Business Suite Client Environment

You can modify, repair or remove the Client Environment installation components by using the Windows Programs and Features application available from the Control Panel window.

Note: *The Component Enabler installation only provides for the removal of the application. Modify or Repair are not available options.*

To perform any of these functions, perform the following:

1. Point to and click the **Start** icon in the bottom-left corner of the screen.
2. Right-click a blank part of the **Start** screen and then select **All apps**. Select **Control Panel** from the **Apps** screen to display the Control Panel window.
3. Select **Programs and Features** to display the Programs and Features dialog box listing all the installed programs.
4. Locate the program that you want to remove, from the list and click **Change/Remove** to display the Setup Maintenance dialog box.

5. Click the **Change/Repair/Uninstall** option for the operation that you wish to undertake.
6. Click **Next** to continue with the selected operation.

The available maintenance operations are shown below.

Change

Change allows you to add Client Environment components that were not installed during the original installation, or remove selected components via the Feature Selection Screen.

If you select the Change operation, when you click **Next** and no hotpatch exists, the Feature Selection dialog box is displayed. From the list of components select the ones that you wish to add, or deselect the ones that you wish to remove.

If a Hotpatch is already installed, then a message box is displayed to request that you manually uninstall the Hotpatch prior to continuing with the modification. Click **Confirmation** to terminate the maintenance. You must then uninstall the hotpatch before recommencing with the modification. After the modification is complete, you should re-install the Hotpatch.

Repair

Repair the Client Environment installation by reinstalling all non-customizable files in the same location as the previous installation. If any of the files were accidentally deleted or modified, then this option restores the software back to its original state.

If you select the Repair operation, when you click **Next**, and no hotpatch exists, the installation proceeds automatically.

If a Hotpatch is already installed, then a message box is displayed to request that you manually uninstall the Hotpatch prior to continuing with the modification. Click **Confirmation** to terminate the maintenance. You must then uninstall the hotpatch before recommencing with the modification. After the modification is complete, you should re-install the Hotpatch.

Uninstall

Remove all non-customizable Client Environment files and remove all the registry entries. This restores the computer to the state prior to installation of the Client Environment. If a Hotpatch is already installed, the setup program automatically uninstalls the Hotpatch before uninstalling the Client Environment.

If you select the Uninstall operation, when you click **Next**, a message box is displayed requesting you to confirm or cancel the operation. If you confirm the operation, the Client Environment is uninstalled.

Section 6
Runtime for Windows ® Operating System Installation

This section describes how to install Agile Business Suite Runtime for the Windows Operating System.

Required System Software Configuration

The system software configuration required to support Agile Business Suite Runtime for Windows is detailed in the table below.

Required Item	Comments
• Windows Server 2016 Standard, Datacenter (LTSC) v1607 • Windows Server 2022 Datacenter Edition (latest update)	Windows 10 is not supported on the AB Suite Windows Runtime production environment, but can be used for testing purposes. You require latest updates for testing. Other Windows Operating System editions, such as Home or Server Core Editions are not supported and might not work with AB Suite 7.0 Runtime for Windows. AB Suite 7.08.0 currently supports 64-bit Windows 10 (1909 version) , Windows Server 2016 (LTSC versions), and Windows Server 2019 (LTSC versions) only. It does not support 32-bit Windows. Windows Server Semi-Annual Channel versions, such as version 1803, and 1809 are not currently supported.
Qualified for .NET Framework 4.7.2	This is a requirement for all features. .NET Framework 4.7.2 or later is required for AB Suite Runtime for Windows.
Internet Information Services	The version of IIS depends on the operating system that you are using. Refer to your Microsoft information for the appropriate version. This requirement is only needed for certain features.
Message Queuing	This requirement is only needed for certain features.

Required Item	Comments
• SQL Server Enterprise Edition 2017 or • SQL Server 2017 Express, Developer, Standard Edition	AB Suite 7.0 Runtime for Windows currently supports SQL Server 2017 only. It does not support SQL Server Express and Developer Editions. These can be used for testing purposes only. You require the latest updates for testing. This requirement is only needed for the database server.
Microsoft Visual C++ Redistributable for Visual Studio 2017	This requirement is a must for installing Agile Business Suite 7.0 for Window Runtime on a Windows server. You can install the runtime without Developer or Visual Studio 2017. However, the Runtime is dependent on Visual Studio 2017 runtime libraries, which are freely available. You can download these libraries from: https://support.microsoft.com/en-in/help/2977003/the-latest-supported-visual-c-downloads ***Note:*** *x86 redistributables are still required on an x64 bit machine. You should install these Visual Studio 2017 runtime components before installing the GCA.* Visual C++ for Visual Studio 2017 is also required as some parts of AB Suite 7.0 Runtime for Windows are built using Visual C++.
Microsoft OLE DB Driver for SQL Server	This is a requirement for all the Runtime features. AB Suite uses the TLS 1.2 features that come with the new Microsoft OLE DB Driver for the SQL Server to provide better security during Windows Runtime and Debugger sessions.

Minimum Hardware Requirements

This section describes the minimum recommended hardware requirements for running Runtime for Windows.

Hardware	Runtime
Processor	4 core, 2 GHz
Memory	8 GB RAM
Disk space	200 GB
Monitor	LCD

Note: *Check with your vendor for the dependent software disk space needed. Your disk space allocation on the Windows operating systems server for Runtime should be based on the following approximate allocation of disk space:*

- *226 MB Agile Business Suite Developer software*
- *25 MB Agile Business Suite Runtime software*
- *20 to 50 GB Visual Studio 2017 software minimum installation*
- *6 GB SQL Server 2017 software minimum installation*
- *Actual disk space requirements for SQL Server database files depends on database use. (Remember to allow space for the databases to grow, if needed.)*

Installing Runtime for Windows

Agile Business Suite Runtime for Windows can be installed on any workstation or as a network installation with shared components. All installation types are detailed in this document. When you are installing Runtime for Windows, it appears as the following software modules:

Module	Description
Runtime	Installs runtime core, deploy server and shared components. Requires .NET Framework 4.7.2.
AdminTool	Installs the client administration tool as a Microsoft Management Console “snap in”.
DB Migrate Utilities	Installs only database migration tool components. The AB Suite Runtime infrastructure is not installed with the DB Migrate Utilities. It requires Microsoft SQL Server 2017 Integration Service package.

Notes:

- *You can install AB Suite 7.0 Runtime with the earlier versions of AB Suite Runtime, such as AB Suite Runtime 6.1, 5.0, 4.0, 3.0, and 2.0*
- *You can install AB Suite 7.0 Runtime with AB Suite 7.0 Developer only.*

COM+ Network Access in Windows 10 and Windows Server 2016

In the Windows 10 and Windows Server 2016 operating systems COM+ network access is enabled in the windows registry by enabling a registry key and not through the Add Roles and Features wizard of the Server Manager window.

Caution

The registry key must be enabled by experienced administrators only.

To enable a registry key in the windows registry

1. Open the Registry Editor window by performing either of the following:

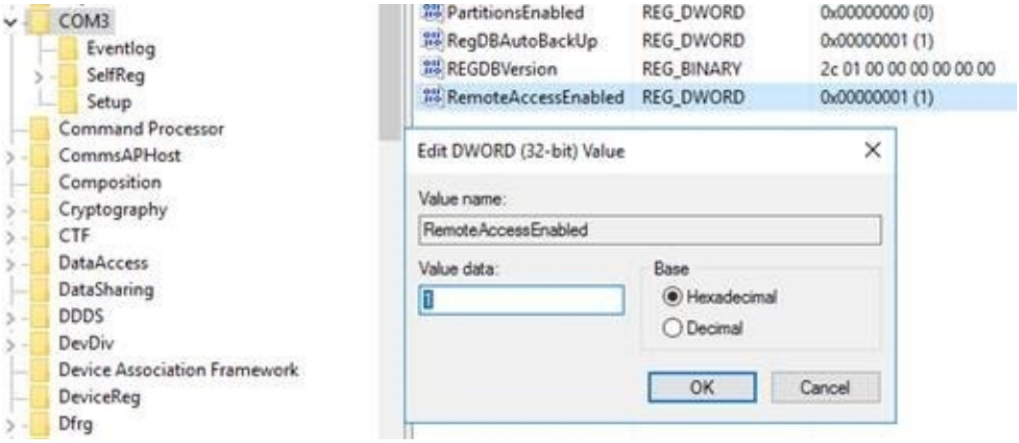
   a. In the search box on the task bar, enter regedit and select **regedit** from the list.

   b. Right-click **Start** and then select **Run**. In the Run window, enter regedit and click **OK**.

2. In the **User Account Control** dialog box, click **Yes**.

   The Registry Editor window appears.

3. Navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3.



PartitionsEnabled	REG_DWORD	0x00000000 (0)
RegDBAutoBackUp	REG_DWORD	0x00000001 (1)
REGDBVersion	REG_BINARY	2c 01 00 00 00 00 00 00
RemoteAccessEnabled	REG_DWORD	0x00000001 (1)

Value name: RemoteAccessEnabled

Value data: 1

● Hexadecimal

○ Decimal

009050

4. Double-click RemoteAccessEnabled.

   The **Edit DWORD (32-bit) Value** dialog box appears.

5. In the **Value data** text box, enter 1.

6. Click **OK**.

Setting up User Accounts

Prior to installing Runtime, you must set up and configure user accounts for “Application User” and “Application Administrative User”. The installation will ask for the name, domain, and password of these accounts. The installation checks that the accounts exist and verify the credentials supplied. These credentials are then used to initially configure the identities of those components that are required to run as the Application User, or the Application Administrative User.

Refer to Configuring User Accounts for more information about the configuration details that might need to be applied for these user accounts after installation.

Unisys Installation Interface

When you double-click the RuntimeCDBrowser.exe, the Unisys Installation Interface appears. The Unisys Installation Interface controls the installation process and indicates the product name. When this interface appears, the installation program checks if you have administrative rights on the machine, and if your machine has the required operating system. If any of these checks fail, a message box appears and you are prompted to terminate the installation.

If the checks are successful, a welcome dialog box is displayed, click **Next**. It is followed by a license dialog box. Click **Accept** on the license dialog box, if you want to continue with the installation.

You are then given the opportunity to select the type of installation that you wish to initiate, and to select the target drive and directory for the installation if you do not wish to accept the default installation location.

The options are:

- **Complete**

  Select this option to install all components of Runtime.

- **Custom**

  Select this option to display the Select Features dialog box to allow you to select the components that you wish to install.

Custom

When you select the **Custom** option from the Installation Interface, the Select Features dialog box is displayed which provides the following options:

- Runtime
- AdminTool
- DB Migrate Utilities

Runtime

Select this option to install the Runtime software, which includes runtime core, deploy server and shared components.

When you install core runtime, protocol adapters are automatically installed. The following protocol adapters are installed:

- RATL over TCP/IP – this is a legacy protocol that is used by version 3.x of Component Enabler.
- RATL over MSMQ – for Component Enabler to use Remote Access Server (RATL) over MSMQ.
- SOAP over HTTP (Web Services) – SOAP over a HTTP connection is the current standard.

- SOAP over MSMQ – uses the SOAP adapter to call over MSMQ.
- HUB - a proprietary protocol that allows other Agile Business Suite systems to talk to each other.
- NOF/OFF/USER/GLI – proprietary protocols that are mainly used to migrate applications from mainframe hosts to Windows hosts.

AdminTool

Select this option to install the client administration tool as a Microsoft Management Console "snap in".

DB Migrate Utilities

Select this option to install the utilities for managing your database.

The database migration utility option comprises EAE DBMigrate Utility SQL 2017. The DBMigrate Utility version used must match the target SQL Server instance version. For example, if the SQL Server version is SQL Server 2017, then you must use DBMigrate for SQL 2017 Utility.

Note: *If you are using an older version of SQL Server, you must back up the runtime database and then restore it into the target SQL Server instance, before running the DBMigrate Utility. For example, if the target is SQL Server 2017, then restore the EAE database backup into SQL Server 2017 before running DBMigrate for SQL Server 2017 Utility.*

The Microsoft SQL Server Integration Service (SSIS) package is required for runtime data migration from one version to another. Therefore, for installing EAE DBMigrate Utility SQL 2017, you must install SQL Server 2017 Integration Service package. Refer to http://msdn.microsoft.com/en-us/library/ms143731.aspx for more information on installing SSIS.

In the Runtime Installation wizard, when you select Complete Installation, the installer verifies if SQL Server 2017 Integration Service Package is available and displays the appropriate warning message as follows

- Scenario 1: When SSIS for SQL Server 2017 is not available, the installer displays a warning message to install SSIS for SQL Server 2017 before continuing with the installation of the DBMigrate sub-features.
- Scenario 2: When SSIS for SQL Server 2017 is available, the installer displays a message to install the DBMigrate custom component in the SQL Server 2017 directory. Click **OK** to install all the sub-features; else click **Cancel**.

In the Runtime Installation wizard, when you select SQL Server 2017 DBMigrate, the installer displays a message to install SSIS for SQL Server 2017 if it is not available. If it is available, the installer displays a message to install a custom component in the SQL Server 2017 directory. Click **OK** to install the DB Migrate for SQL Server 2017; else, click **Cancel**.

Completing the Installation

After you select the components that you want to install, click **Next** to display the Start Copying Files Screen. This allows you to review the installation settings before completing the installation. This screen displays the components that are selected and the installation directory. If you are satisfied with the settings, click **Next** to proceed with the installation, otherwise click **Back** to make changes.

The installation then checks to see if the required level of Microsoft Visual Studio .NET Framework exists on the machine, then the installation proceeds, otherwise a warning message is given and you are asked to terminate the installation.

At the completion of the installation, the Installation Complete Screen appears. This screen displays the following options:

- **Update Runtime in PATH environment variable** – adds the AB Suite Runtime installation path to the system PATH variable when you select this check box and click **Finish**. You can clear the check box if you do not want to add the AB Suite Runtime installation path to the system PATH variable.

  Note: *The benefit of adding the AB Suite Runtime folder to the PATH is that utilities such as the RUNREP executable will be more easily found and can be executed without full path qualification. If you have multiple versions of AB Suite Runtime installed side-by-side then you should not add the runtime folder to the PATH environment variable as this might result in the wrong executable files being accessed at runtime.*

  This check box is selected by default.

- **Show the readme file** – displays the readme file when you select the check box and click **Finish**. You can clear the check box if you do not want to view the readme file. This check box is not selected by default.

- **Show the Windows Installer log** – displays the AB Suite <version> Runtime.log file when you select the check box and click **Finish**. You can clear the check box if you do not want to view the log file. This check box is not selected by default.

Click **Finish** to complete the installation.

Silent Installation

The Windows Runtime Installation Package has the extension .msi and the Silent Installation can be run using the msiexec.exe utility. When the command line argument "/qn" is passed to the utility, it installs the Windows Runtime Installation Package without Graphical User Interface (GUI) that is, no dialog boxes, no user prompts requesting information (Install directory). The progress of the installation whether the installation has completed successfully or failed is written to a log file. The log file includes the status, warning and error messages.

Implementation of Silent Installation

From the command prompt, executing the following command line arguments “:> msiexec.exe /i “<path of the AB Suite 7.0 Runtime.msi>\AB Suite 7.0 Runtime.msi” /qn <parameters> installs the Windows Runtime Installation package in silent mode.

The purpose of the Silent Installation is to automate the installation without Graphical User Interface (GUI) of Windows Runtime Installation. This means, no dialog boxes, no user prompts requesting information is displayed to the user.

Processing

The command and parameters to execute the AB Suite packages are as follows:

Commands/Parameters	Values
msiexec /i	Example: <default directory>\AB Suite 7.0 Developer\Product Configuration 1\Release 1\DiskImages\Disk1\AB Suite 7.0 Developer.msi
/qn INSTALLDIR =	Example: C:\Program Files\Unisys\AB Suite 7.0\
AgreeToLicense	Yes
ADDLOCAL	ALL
APP_USER_DOMAIN=	.
APP_USER_NAME=	Example: AppUser
APP_USER_PASSWORD=	Example: App1User
APP_ADMIN_DOMAIN=	.
APP_ADMIN_NAME=	Example: AppAdminUser
APP_ADMIN_PASSWORD=	Example: App1AdminUser
PASSDATA=	Example: C:\AB Suite 7.0\Data\
PASSBUILDERCACHE=	Example: C:\Program Files\Unisys\AB Suite 7.0\Builder Cache\
PASSBUILDEROUTPUT=	Example: C:\Program Files\Unisys\AB Suite 7.0\Builder Output\
/l*v	Example: C:\Temp\AB Suite 7.0.Log

Where,

msiexec is the executable program of the Windows Installer to interpret installation package and install products on the target location.

/i switch is used to install the package from the command line.

INSTALLDIR is a property for specifying the location where the Windows Runtime Installation Package is installed.

/qn switch is used to suppress the dialog boxes displayed for input and output to the user.

/l*v switch is used to create a log file.

For example, to install Runtime through Silent Installation, run the following command from the command prompt:

```
msiexec /i "Agile Business Suite 7.0 Runtime (64 bit).msi" /qn /norestart INSTALLDIR=
"C:\Program Files\Unisys\AB Suite 7.0\" AgreeToLicense=Yes ADDLOCAL=ALL APP_USER_DOMAIN=.
APP_USER_NAME=AppUser APP_USER_PASSWORD=App1User APP_ADMIN_DOMAIN=.
APP_ADMIN_NAME=AppAdminUser APP_ADMIN_PASSWORD=App1AdminUser
PASSDATA="C:\AB Suite 7.0\Data" /l*v c:\temp\Runtime.log
```

Uninstall Agile Business Suite Runtime

You can uninstall the AB Suite Runtime from the Control Panel.

To uninstall the AB Suite Runtime, perform the following

1. Open **Programs and Features** from **Control Panel**.
2. From the list of installed programs, right-click **Agile Business Suite Runtime**, and then select **Uninstall**..
3. Click **Yes** when prompted to confirm and continue with the operation.

   Click **No** if you do not want to uninstall the AB Suite Runtime.

Section 7

Runtime for Windows® Operating System Configuration

This section provides details of the configuration required in setting up the Runtime for Windows Operating System environment.

Configuring User Accounts

Runtime requires two users to be created, under whose identities the various operations will run.

The Application User's identity is used for the standard operations and has a lower privilege level. The Application Administrative User's identity is used to perform administrative tasks for which a higher privilege level is required.

Refer to Preparing for Installation of Agile Business Suite for more information on how to create and configure the user accounts.

These users must be created prior to installation. It is up to the system administrator to decide which accounts are used to represent the Application User and the Application Administrative User.

The User accounts must be granted access to the server as described in Server Configuration.

The Application User

The Application User has a normal Windows operating system user account from either the local or network domain, to which the following rules apply:

- The user account is required to have direct or indirect membership of the local "Users" group, or its equivalent.
- The account name must not contain any blanks.
- The account must not have a blank password.
- The account password must not contain any blanks.

The Application User account must be a domain account, if any of the following conditions are true:

- The application would be accessed by any end-user via a domain user account. The processes running as the Application User needs to verify the membership of users in various COM+ Roles. This cannot be done for domain users unless the Application User is also the domain user.
- The database is on a different machine to the application.
- The RATL/MSMQ protocol is used.
- The SOAP/MSMQ protocol is used.
- A printer that is to be used is on a different machine to the application.
- The protocol adapters are running on a different machine to the application, and the RATL, HUB, RATL/MSMQ, SOAP/MSMQ, or SOAP/HTTP protocol is to be used.

The following processes run under the Application User identity:

- The process housing the RATL protocol adapter.
- The process housing the RATL/MSMQ protocol adapter.
- The process housing the SOAP/MSMQ protocol adapter.
- The process housing the SOAP/HTTP protocol adapter.
- The process housing the HUB protocol adapter.
- The processes housing the applications.
- The process housing the generated reports.
- The process housing the Report Session Manager.

Application User Account Required Rights and Privileges

The account should not be granted any privileges beyond those specified below.

On all machines:

- The “Log on as a batch job” required due to some batch processes assuming the Application User’s identity.
- Log on as a service

On the machine hosting the protocol adapters:

- Log on as service is required to be able to log into the gateway services on the machine.

On the machine hosting the databases, when the databases are on a different machine to the applications:

- "Access this computer from the network" required in order to connect to the database remotely.

On Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems

With Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems, the User has to be explicitly added to COM+ Users Role. Everyone logging in must be in the COM+ Users Role. By default, only the Administrators Group is added, but with Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems, it is only the Administrator version of those users, not the Standard User version that are members of the Administrators Group. Therefore, no Standard User accounts are added by default into the Users Role. In earlier versions of Windows, the user was automatically in the Users Role via its membership of the Administrators Group. Non-administrative users still had to be added manually to the Users Role. In Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems, this rule still applies, but now everyone is a non-administrative user by default.

The Application Administrative User

The Application Administrative User has a normal Windows Operating System user account from either the local or network domain. It is required to have direct or indirect membership of the local "Administrators" group, or its equivalent.

The Application Administrative User account must be a domain account if any of the following conditions are true:

- The application would be accessed by any end-user via a domain user account. The processes running as the Application Administrative User needs to verify the membership of users in various COM+ Roles. This cannot be done for domain users unless the Application Administrative User is also the domain user.
- The database is on a different machine to the applications.
- The applications are deployed remotely.

If the Application Administrative User account is a domain account, then it must **not** have a roaming profile.

In addition, if applications are to be deployed remotely, the Application Administrator User's account must be marked as "Account trusted for delegation" in the domains active directory. This applies only to Windows 2010 and later, domains. The change might not be immediately visible as it can take some time to propagate throughout the machines within the domain. This is applicable for all the supported operating systems. Therefore, the deployment server running as the Application Administrative User impersonates the user that invokes the deployment to access the resources on the developer machine. This requires the invoking user to be given the administrator privileges in the runtime server and the Application Administrative User to be given the "Account trusted for delegation" privilege.

Note: *In Windows Server 2010 and later version domains, to provide delegation privileges to the Application Administrator User account and mark it as "Account trusted* *for delegation", you should assign Service Principal Name (SPN) to the Application Administrator User account in the active directory.*

For example, to assign an SPN name 'https/AppAdminUser' to AppAdminUser account, run the following setspn command on domain controller:

```
setspn –a https/AppAdminUser AppAdminUser
```

where, the first parameter, https/AppAdminuser, is an SPN name and the second parameter, AppAdminUser, is an account name. You can also prefix a domain name with the account name, for example,

```
setspn –a https/AppAdminUser MyDomain\AppAdminUser
```

The RuntimeServiceImpersonationLevel registry key provides an alternate method of deployment. With this registry key, you can choose to deploy a system with or without the Application Administrative user having delegation privileges. The RuntimeServiceImpersonationLevel is of the type String and is stored in the runtime machine under the following registry key:

```
\HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Unisys
   \AB Suite
    \7.0
     \SM Runtime
```

where

```
"RuntimeServiceImpersonationLevel"= string:"Anonymous/Delegate"
```

Note: *The registry setting must be reapplied after each IC upgrade.*

The RuntimeServiceImpersonationLevel registry key can be assigned the following values that represent various impersonation levels:

- Anonymous (Security Anonymous) – When you assign the Anonymous value, the deployment process is initiated by using the Application Administrative User account instead of the user that invokes the deployment process. This avoids the Application Administrative User to be given the "Account trusted for delegation" privilege. Additionally, the user that invokes the deployment does not need to be given the administrator privileges in the runtime server. However, the invoking user must be part of the "Security Administrators" COM+ role under security helper and the "Deployers" COM+ role under deployment server.
- Delegate (Security Delegate) – When you assign the Delegate value, the deployment process is initiated by the user that invokes the deployment process. By default, the impersonation level is set to the Delegate value.

WARNING

Since runtime cannot identify or authenticate the user, who deploys a system, any anonymous user can deploy a system. The anonymous user who invokes the deployment need not be given the administrator privileges in the runtime server. However, the invoking user must be part of the "Security Administrators" COM+ role under security helper and the "Deployers" COM+ role under deployment server. Additionally, the administrators cannot trace the users who have tried to deploy and access the runtime server resources.

By default, the setting is Delegate.

Refer to the *Agile Business Suite Developer User Guide* for more information on deploying with reduced impersonation levels.

Client and server(s) taking part in remote deployment, as well as the client user, and Application Administrative User, must all be part of this domain.

The following processes run under the Application Administrative User identity:

- The process housing the Database Configuration application.
- The process housing the Database Reorganization application.
- The process housing the Runtime Manager.
- The process housing the System Administration application.
- The process housing the Security Helper application.
- The process housing the Deployment Server.

Application Administrative User Account Required Rights and Privileges

The account should not be granted any privileges beyond those specified below.

On all machines:

- "Log on as a batch job" required as some batch processes assumes the Application Administrative User's identity.

On the machine hosting the applications:

- "Replace a process level token" required to run deployment packages and make external calls.
- "Act as part of the operating system" required to verify all domain user credentials. This privilege is also needed for deployment operations using the non-console Remote Desktop Connections on both operating systems.

On the machine hosting the databases when the databases are on a different machine to the applications:

- "Access this computer from the network" required to be able to connect to the database remotely.

  With Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems, it is only the Administrator version of those users, not the Standard User version that are members of the Administrators Group. Therefore, no Standard User accounts are added by default into the Users Role. In earlier versions of Windows, the user was automatically in the Users Role via its membership of the Administrators Group. Non-administrative users still had to be added manually to the Users Role. In Windows 10, Windows Server 2016, Windows Server 2019, and higher Operating Systems, this rule still applies, but now everyone is a non- administrative user by default.

Changing Passwords

There might be occasions when it is necessary to change the passwords for the Application User or Application Administration User accounts. When changing the password manually, it must be changed in the following places:

- The required User account; either Application User or Application Administration User.
- The process identities. All processes running under the User identities need to have their configurations updated with the new password. Refer to The Application User and The Application Administrative User, for list of these processes.

In addition, the Change Database User Password Tool needs to be used to change the Database User's password for all database users. Refer to Change Database User Password.

Changing Accounts

It is recommended that the Application User and Application Administrative User accounts not be changed once they are setup. If an account needs to be changed in any way, whether it is simply renamed or an entirely new account is created, all references to the old account must be manually replaced. References in the following places must be updated:

- All Agile Business Suite processes running with the identity of the changed account, as listed in The Application User and The Application Administrative User.
- All COM+ roles referring to the changed account.
- If the account is recreated, as opposed to renamed, the data files folder needs to have its permissions reset to allow Full Control to the changed account.
- If the account name is recreated, as opposed to renamed, the SID of User account needs to be stored in flat files for Application User and Application Administrative User. They are created in the Data\Private directory. For example:

  ```
  AB Suite 7.0\Data\Private\Security\Users\Application User
  AB Suite 7.0\Data\Private\Security\Users\Application Administrative User
  ```

The SID of the Application User is stored in the Application User file and the SID of the Application Administrative User is stored in the Application Administrative User file.

SQL Server Specific

- The SQL Server login used by the Application User needs to be reconfigured to allow access to the changed account with the appropriate permissions.
- The SQL Server databases used by Agile Business Suite needs to grant the changed account access as a user of the database, and if the changed account is for the Application Administrative User, include it in the db_owner role.
- The SQL Server users utilized by Agile Business Suite in the databases need to have their passwords changed using the Change Database User Password tool. Refer to Change Database User Password.

Change Database User Password

When the Application User and Application Administrative User accounts are changed or their passwords altered, you need to change the passwords of any affected database users. To Change the Database User Password:

1. Open the Administration Tool.
2. Right-click the system node.
3. From the context menu, click **All Tasks** > **Change DB Password**. The **System Schema Account Password** dialog box is displayed.
4. Enter the new Account Password.
5. Re-enter the new Account Password in the **Confirm Password** field.

   Note: *Do not use the following characters when changing database schema password as these characters are not allowed in a SQL connection string:*

   *[] () , ; ? * ! @ =*
6. Click **Apply** and **OK** to change the DB Server user password.

Note: *If you have multiple runtime server instances accessing the same DB Server, you must coordinate the passwords manually. The **Database Login Password Change Option** is selected by default. This option allows you to automatically update the password for the DB Server instance, if the user id has sufficient privileges. Otherwise, the DB administrator can manually update the password for the SQL Server instance.*

Server Configuration

SQL Server

The SQL Server must be configured as follows:

- Allow both SQL Server and Windows authentication (Mixed Mode).
- Use the Local System account in the Services Accounts screen.
- Select Latin1_General Accent-sensitive for the Collation settings.

The Application User must be granted a SQL Server login to the database server that is to be used by Agile Business Suite. The login is case-sensitive and must be in the same case as specified in the Windows Security Accounts Manager database.

Notes:

- *The imported Model database has to be this collation sequence of LATIN1_General_CI_AS because it is case-sensitive considering LDL is casesensitive as well. If the imported Model has a different collating sequence, AB Suite might function unpredictably. Also, note that this collating sequence does not affect Kanji because it uses Unicode for most strings.*
- *Also note that the System Modeler always creates its repository with the collation sequence it requires regardless of the SQL Server Instance default, which is Latin1_General_CI_AS. Runtime Administrators are free to install SQL Server under any kind of collation sequence database they like and Admin Tool can prepare it for use for Runtime.*
- *Some Servers, which have non English locales might require a different collation sequence. Contact your CSC to determine the best collation sequence for your locale. For example, a Latvian locale requires the Latvian_100_Bin.*

Configuring the Default ‘sa’ Account

When SQL Server is installed, by default the ‘sa’ account is created with a blank password. In order to ensure that unauthorized users do not gain access to your server, it is recommended that you assign a password to the ‘sa’ account. If a password is not assigned and an unauthorized user gains access using the ‘sa’ account, they will have full control of all databases contained on your server.

Runtime Server Configuration

If you are using EOM printing on a Windows 2019 Server, ensure that the **Untrusted Font Blocking** Group policy is disabled on the printer server. If this policy is enabled on the printer server, printed documents may be completely or partially blank, because the operating system is unable to render untrusted (non-default) fonts.

The following link from Microsoft confirms that it is safe to disable this policy with the latest Windows security:

Untrusted Font Blocking

User Profile Service Configuration

The default behavior of the User Profile service can lead to problems for the AB Suite Windows Runtime system running on a server. This is due to the user registry setting being prematurely unloaded by the operating system resulting in

- The AB Suite Windows Runtime system becoming unresponsive.
- The Windows Application event log displaying the following error:
  - 0x800703fa : Illegal operation attempted on a registry key that has been marked for deletion
- The AB Suite Windows Runtime System log displaying the following error:
  - ReportSessionManager(13264:21080) [Domain\Appuser]; COM Error -2147467259 occurred in :: class CRunningSystem *__cdecl CConfigurationAgent::ConfigDataForSystem(wchar_t *const)

The solution is to enable the following User Profile setting:

- Do not forcefully unload the user registry at user logoff.

To modify the User Profile setting, perform the following:

Prerequisites:

- From Component Services, shut down all the running AB Suite COM+ processes.
- From Services, stop all the AB Suite services.
- Ensure that there are no processes running under AB Suite Application User or Application Administrative User.

1. Open the Local Group Policy Editor.

   You can open the Local Group Policy Editor through Run.

   - Start **Run** using Windows+R, type **gpedit.msc**, and click **OK**.

2. In the left pane, expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, and then select **User Profiles**.

   The User Profiles appear in the right pane.

3. Under Setting, select **Do not forcefully unload the users registry at user logoff**.
4. Click **policy setting** to edit the User Profile.

   The Do not forcefully unload the users registry at user logoff window appears.

5. Select **Enabled** and click **OK**.
6. Restart the Runtime server.

Note: *The procedure to configure User Profile service applies to Windows 10, Windows Server 2016, and Windows Server 2019.*

User Configuration

Client Users

Users accessing an Agile Business Suite application through a client must be authenticated on the machine(s) containing the protocol adapters and applications.

If the protocol adapters and applications are located on the same machine, then the client user requires only a local account.

If the protocol adapters and applications are located on different machines communicating via a network, then the client user requires a domain account.

Regardless of the location of the protocol adapters and applications, the client user's account must have the "Access this computer from the network" option set on the host machine(s), in order to be able to logon.

In order for the client to access an application, the user must be added to the "Users" role on the COM+ application containing the Agile Business Suite application.

Administrative User

Administrative users are those users who are permitted to access applications for administrative purposes. These users are authorized to perform administrative tasks according to the COM+ roles to which they belong.

Note: *With Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems, it is only the Administrator version of those users, not the Standard User version that are members of the Administrators Group. Therefore, no Standard User accounts are added by default into the Users Role. In earlier versions of Windows, the user was automatically in the Users Role via its membership of the Administrators Group. Non-administrative users still had to be added manually to the Users Role. In Windows 10, Windows Server 2016, Windows Server 2019, and later Operating Systems, this rule still applies, but now everyone is a non-administrative user by default*

The following table outlines the available COM+ roles and the administration commands to which they grant access. Refer to the *Runtime Administration Tool Online Help*for more information on how to use the administration commands.

COM+ Roles	Administration Commands
Accountants	HighAccountMonth
	LowAccountMonth
Application Administrators	DeleteReportRecovery()
	HighAccountMonth

COM+ Roles	Administration Commands
	IsHubEnabled
	GetHubStats()
	GetRecoverableReports()
	GetRunningReports()
	ListIspecs()
	LowAccountMonth
	RecoverReport()
	RunReport()
	SendAMessage()
	SetSessionInfo()
	StopReport()
	StopSystem()
	WakeUpReport()
Application Operators	ListIspecs()
	SetSessionInfo()
	StopSystem()
Hub Administrators	GetHubStats()
	IsHubEnabled
Hub Monitors	GetHubStats()
Message Broadcasters	SendAMessage()
Message Senders	SendAMessage() (Unicast only)
Report Administrators	DeleteReportRecovery()
	GetRecoverableReports()
	GetRunningReports()
	RecoverReport()
	RunReport()
	StopReport()
	WakeUpReport()
Report Monitors	GetRecoverableReports()
	GetRunningReports()
Report Operators	GetRunningReports()

COM+ Roles	Administration Commands
	StopReport()
	WakeUpReport()
Report Recoverers	GetRecoverableReports()
	RecoverReports()
Report Recovery Administrators	DeleteReportRecovery()
	GetRecoverableReports()
	RecoverReport()
	WakeUpReport()
Report Recovery Operators	DeleteReportRecovery()
	GetRecoverableReports()
	WakeUpReport()
Report Runners	DeleteReportRecovery() (Own reports only)
	GetRecoverableReports() (Own reports only)
	GetRunningReports() (Own reports only)
	RecoverReport() (Own reports only)
	Run Report()
	Stop Report() (Own reports only)
	WakeUpReports() (Own reports only)

Note: *The BUILTIN\Administrators group requires authentication with the domain authority, so if you wish to add this group to any COM+ roles, you must ensure that you have installed AB Suite 7.0 GCA using the domain level credentials for Application Users and Application Administration Users. Installing the product using local user accounts results in incorrect behavior for role based authentication.*

Configuring Runtime for Normal users

This subsection discusses about configuring AB Suite Runtime so that normal users without administrative privileges can access the Runtime administration tasks. AB Suite Runtime uses the "AB Suite Runtime Administrators" user group on the local machine to allow non-administrative users to access the Runtime administration tasks. By default, the user group does not have administrative privileges. This user group is automatically created on installing AB Suite Runtime, if it does not exist, and removes the user group upon uninstallation of AB Suite Runtime.

WARNING

Allowing access to administrative functionality for non-administrative users is not recommended, as it allows a non-administrative user to perform actions that are normally restricted for system security. You must be aware that the membership of the AB Suite Runtime Administrators group indirectly allows access to the protected system resources.

To view the "AB Suite Runtime Administrators" user group, perform the following:

1. Open Computer Management, accessible from the Administrative Tools folder in the Control Panel.
2. From the Tree view, expand **System Tools**, **Local Users and Groups**, **Groups**.

Adding New Non-administrative User to Access Runtime

To allow a new non-administrative user to access the AB Suite Runtime administration tasks, an administrator should add the new or existing user to the "AB Suite Runtime Administrators" user group by using the Component Services MMC snap-in. This allows members of this group to access the AB Suite Runtime administration tasks. By default, the "AB Suite Runtime Administrators" user group is automatically added to the "Runtime Administrators" COM+ role of the Runtime Manager application and the "Deployer" COM+ role of Deployment Server application.

Securing the Runtime Administration Tasks

If a user is not an administrator of the remote server machine, security configuration is required for performing the Runtime administration tasks. To access

- ConfigureLog.exe and ConfigureAdapter.exe, all users must be made part of the "Runtime Administrators" COM+ role of the Runtime Manager component by using the Administration Tool. This can be achieved by adding new users in the "AB Suite Runtime Administrators" group. You can add all the users in the "AB Suite Runtime Administrators" group by using the Component Services MMC snap-in.
- Deploy.exe, all users must be made part of the "Deployer" COM+ role of the Deployment Server component by using the Administration Tool.

  The non-administrative users in the "Deployer" COM+ role cannot perform deployment operations, even if they are added to the "AB Suite Runtime Administrators" group. All users must have local administrator privileges to perform the deployment operations.

Refer to Command Line and Programmatic Access to Runtime in the *Agile Business Suite Runtime for Windows® Operating System Administration Guide* for more information about the user privileges.

Other Security Considerations

Protecting Your Network Traffic

Since Runtime does not enforce network security, except between the Runtime components themselves, it is recommended you adopt some kind of protection for your information transfers. There are a number of technologies available to protect network traffic, such as IPSec and TLS 1.2.

Deployment

Since the deployment packages are installed in the context of the deploying user, this user must be an administrator on the machine on which the deployment packages are to be installed.

Remote Deployment

It is important that the user be in at least a Windows domain and the user's account not to be marked as "Account is sensitive and cannot be delegated".

Debugger

Debugger requires access to the database in order to run.

If a user is not an administrator of the remote server machine, security configuration is required for the COM+ Security Helper application. All the users using debugger must be part of Secure Users role of Security Helper on the database server. To do this, add all the users to the Debugger Users group. This setting is required when the database server is installed in a separate or in the same remote machine with developer. Users can be added to COM+ roles using the Component Services MMC snap-in.

Runtime Setup

Before you generate an application to a Runtime environment, there are several setup requirements that must be completed. You need to:

- Add a runtime server
- Add a database server registration
- Add a database
- Install the Report Output Control System (optional).

Each of these requirements can be completed using the Runtime Administration tool, with the exception of the installation of the optional Report Output Control System. Refer to the *Runtime Administration Tool Online Help* for more information.

Clustering AB Suite Runtime

Applications generated using AB Suite are not Cluster-Aware but can be made to function like Cluster-Aware applications using the Microsoft Windows Server 2016 Cluster management software along with SQL Server 2017 Failover Clusters. This provides a "High Availability" (HA) environment. The SQL Server 2017 AlwaysOn group should also be compatible, but is not currently supported by AB Suite.

Nodes

A cluster comprises of machines or nodes connected to each other. The Cluster software monitors the processes and services running on each Node. The Node that runs a process or service is called the Active Node. The Passive Nodes do not simultaneously run the same process or service. If a Node unexpectedly fails or is intentionally taken down, the Cluster software ensures that the clustered processes and services from the failed Node are switched to another machine in the cluster, where they can restart and continue. This process is referred to as a **failover**.

Virtual IP Address/Network Name

One of the key capabilities of a failover cluster is the elimination of the need for the end user to know which machine or Node is currently active. The cluster management software achieves this with a floating virtual IP Address depending on which machine is the active Node. In AB Suite Windows Runtime, you only need to enter the virtual network name or IP Address of the cluster to access a particular service or process.

Resources

Application services, virtual IP Addresses, machine names, shared storage and devices that are monitored by the cluster management software are called Resources. Related resources are generally grouped together into Resource Groups for easier cluster management.

Dependencies

Some resources need other resources to run successfully. The relationships between resources are known as Dependencies. Dependencies are used to define how different resources relate to one another. These interdependencies control the sequence in which the cluster management software brings resources online and takes them offline.

AB Suite Application and Database Layers

AB Suite provides the optional ability to separate the application layer from the database layer. This allows the Database and Application to reside on different machines. Hence clustering for AB Suite can consist of two separate components, the Application layer and the Database layer. The exact cluster configuration varies as per requirements. You need to create a Resource Group for AB Suite if you use a separate cluster for the Application layer. Otherwise you can have a single cluster where both AB Suite and SQL Server are a part of the same Resource Group and so will fail over together.

Cluster Resource Group Setup

A cluster Resource Group should exist before setting up the various resources for AB Suite. To set up a separate Application layer cluster, a specific AB Suite Resource Group with its own IP Address and network name is needed. Alternatively it is possible to assign the resources to the SQL Server cluster Resource Group.

In the AB Suite Runtime environment, files such as the log file and the configuration file are created and updated. You must ensure that such files that change are always available regardless of the active Node. You can achieve this by defining shared disk resources. For example, the DATA folder that contains the log and configuration file must be assigned to a shared disk resource during installation.

You can do this post installation by changing the registry entries for:

```
HKLM\Software\UNISYS\AB Suite\7.0\SM Runtime
```

or

```
HKLM\Software\Wow6432Node\UNISYS\AB Suite\7.0\SM Runtime
```

if running 64-bit

The 3 keys to update are DataFolder, PrivateFolder, and PublicFolder.

It is also recommended that the application be deployed to a shared disk resource.

AB Suite Runtime Software Installation in a Cluster

Note: *The AB Suite software installation requires that a Microsoft Cluster be created and that a SQL Server environment exists either in the cluster or in a separate cluster environment.*

Since AB Suite applications are not cluster-aware, you have to manually ensure that the same options and configurations are used on each node in the cluster.

To install the basic AB Suite Runtime software, perform the following:

1. Install **AB Suite Runtime**.
2. Configure AB Suite protocol adaptor resources.

3. Define a generic script resource monitor.
4. Set up dependencies.

Installing AB Suite Runtime

It is important to create and add domain level Application and Admin user accounts. The AB Suite Application Admin user should be added to the local Administrators group of each Node prior to installation.

To enable AB Suite to install and function correctly in a clustered environment, the database components reside on the runtime server and not on the database server. The Database Server is identified by a virtual IP Address of the SQL Server cluster.

Before installation, select a Node and ensure that the shared disk resource for the Data folder is online. Perform a custom installation pointing to a local disk location for the software installation folder. Ensure that this location is available on all Nodes.

After installation, start the “Services” MMC plugin from **Administrative Tools** > **Services** and change all the AB Suite services to a start type of “Manual”. You can then move the shared disk resource to the next Node and repeat the process ensuring that the same locations are used for the installation and the Data folder, etc.

Configuring AB Suite Protocol Adaptor Resources

You need to create resources for each of the protocol adapters after installing AB Suite Runtime. At a minimum, this is the **AB Suite RATL TCP/IP protocol adaptor**, but it could also include HUB, RATL MSMQ or the SOAP protocol adaptors.

To create a resource for a protocol adapter, perform the following:

1. Start the Server Manager MMC plug-in, and expand **Features**, **Failover Cluster Manager**, **Machine name**, and the **Services and applications** node.
2. Right-click the required Resource Group, and select **Add a resource**, **Generic Service**.

   The **New Resource Wizard** appears.
3. Select the required Protocol Adapter.
4. Click **Next** on the subsequent screens to create the resource.
5. Click **Finish** after adding the required protocol adapters to the resource group.

Defining a Generic Script Resource

The Failover Cluster software provides a **Generic Script Resource** that is used to monitor and perform a clean-up or preparation of the cluster when a failover occurs. The Generic Script resource is a VB script with several predefined functions that are called depending on the state of a resource. For example, **Online**, **Offline**, **IsAlive**, etc. In the event of a failover of an AB Suite application, all the COM+ services are stopped and the status of the AB Suite applications is set to STOPPED. The ABSClusterMonitor.VBS script is used to monitor and call a standalone executable (ShutdownABS.exe) that shuts down all AB Suite COM+ services.

Note: *Both the Sample Generic Script Resource VB Script and the standalone executable should be placed in the Data\Public folder. This is because the script and the executable expect to reside in this location, rather than it being a requirement of the Microsoft Failover Cluster software.*

To add a generic script resource, perform the following:

1. Start the Server Manager MMC plug-in, and expand **Features**, **Failover Cluster Manager**, **Machine name**, and the **Services and applications** node.
2. Right-click the required Resource Group, and select **Add a resource**, **Generic Script**.

   The **New Resource Wizard** appears.
3. Enter the location and name of the VB Script in the **Script file path** box.
4. Click **Next** to create the resource.
5. Click **Finish** after adding the required script to the resource group.

Note: *If there are issues with the script, the resource fails to Add at this point. Check the Cluster logs via the "Cluster.exe" command line utility. The Log files are in the %windir%\Cluster\Reports folder.*

Setting up Dependencies

Dependencies ascertain that the defined relations between resources ensure that resources are available in the cluster and in the correct sequence.

To create a dependency for a resource, perform the following:

To add a generic script resource, perform the following:

1. Expand the Resource group that holds the resource that needs to be updated.
2. Right-click on the resource and select **Properties**.
3. Select the **Dependencies** tab.
4. Click the line under the **Resource** column for the Resource list, and select a shared disk resource.
5. Click **OK** to add a dependency.

Adding a Runtime Server

The first step in setting up a runtime environment is to identify the servers to be used and add them to the Favorites folder for easy access. There are several ways in which to add a server to Favorites:

- Using the Domain and Network Neighborhood nodes, navigate to the required server.

  Once located, either:

  – Right-click the server node, select **All Tasks** and then **Send to Favorites**.

  – Drag and drop the server node to the Favorites folder.

- Alternatively, right-click the Favorites node and select **Add Server**.

  In the displayed dialog box enter the name of the required server and click **OK**.

Adding a Database Server Registration

Before you can add a database, you must set up the database server registration.

1. Right-click the required server node and select **All Tasks**, **Register Database Server**.

   The **Register DB Server** dialog box is displayed.

2. In the **DBMS registration alias name** field, enter a name to identify the database server registration.
3. In the **Server machine** field, enter the name of the database server. If the database is local, enter localhost. Otherwise, enter the remote database server name. If the database server is in a cluster, enter the database cluster name.
4. In the **Instance name** field, enter the SQL Server Instance name. If the SQL server instance on the database server is the default instance, leave this field blank.
5. Click **OK** to add the database server registration node to the runtime server node.

Adding a Database

Once you have added the database server registration you can start adding databases. There are two ways in which to add a database.

Creating a New Database

The Administration tool provides the functionality to create a basic database on the server. However, it is recommended that you create your own databases using the Enterprise Management tools that come with your database software. This has the advantage of enabling you to fully control the preparation, deployment, and configuration of the database.

To create a new database, perform the following:

1. Right-click the required Registration node, point to **New**, and then select **Database**.

   The **Add a New Database** dialog box appears.

2. In the **Name** box, enter the name of the new database.

Note: *You cannot use any SQL reserved keyword, such as Select, Where, Break, Continue, From, and so on as a database name. For example, if you use"Select" keyword as the database name, the following error message is displayed and the tool might crash:*

"Select:- Incorrect syntax near keyword 'Select'"

Refer to MSDN documentation for more information on SQL keywords.

3. Click **OK**.

Attaching an Existing Database

To add an existing database, you must attach the database to the new Windows Runtime environment using the Administration tool. An existing database can be:

- A SQL server database.
- An AB Suite 2.0, 3.0, 4.0, 5.0, 6.1, or 7.0 runtime environment database.
- An AB Suite 2.0, 3.0, 4.0, 5.0, 6.1, or 7.0 runtime database to be used as new debugger database.
- An AB Suite 2.0, 3.0, 4.0, 5.0, 6.1, or 7.0 debugger database created by another user to be used as new debugger database.

To attach an existing database, perform the following:

1. Right-click the Database Server node and select **All Tasks**, **Attach Existing Database**.

   The **Attach a Database** dialog box is displayed with a list of databases that can be attached.

   Notes:

   - *The list includes AB Suite 2.0, 3.0, 4.0, 5.0, 6.1, or 7.0 runtime environment databases and existing SQL server databases.*
   - *Only the AB Suite runtime database names are appended with "(AB Suite)".*

2. Select a database from the list.
3. Click **OK**.

After attaching the database you can start the AB Suite system.

Installing the Report Output Control System

The Report Output Control System (ROC) is an optional module, which you can install. You can browse or print reports using the Report Output Control system. When you start the ROC system, you temporarily leave your application. ROC is a separate system that controls report output for all applications within a given database.

To install the Report Output Control System, perform the following:

1. Use the Runtime Administration tool to add a Database Server Registration called "default". Refer to Adding a Database Server Registration for more information.

2. Open the Command Prompt window as Administrator and use the Change Directory command to go to the <Installation Directory\ROC> directory. For example C:\program files\Unisys\...\Roc.

3. Run the ROC installation script "InstallRoc.js" contained in that directory, passing the Application User login name, the Application User password, and the Application User domain as parameters.

   The syntax is

   ```
   cscript InstallRoc.js <Application-Users login-name>
   <Application-User password> <Application Users domain>
   ```

   For example:

   ```
   cscript InstallRoc.js AppUser App1User .
   ```

   Note: *The "." period in the example signifies the local machine as a domain.*

   When the script runs, it performs the following actions:

   a. Checks if you have a registration called "default".

   b. Creates a database called "ROCDB", if you do not already have one.

   c. Installs ROC from a RocSystem.msi, after the installation of the Report Output Control System is completed successfully.

   d. Deploys ROC and displays a message after a successful deployment.

Note: *You can use the DeployPackage Runtime API to override the default values in the script to install ROC system.*

For example, the following command run from a command prompt as an Administrator, installs ROC System under a "NonDefault" Database Server registration with "NewROCDB" as its Runtime Database.

```
DeployPackage /L <Absolute path of ROCSystem.msi> /U <Application User Login Name>
/P <Application User Password> /TSN localhost /TDBR NonDefault /TDBN NewROCDB
```

Database Configuration

The Runtime Administration tool provides the basic facilities for creating and configuring SQL Server database. However, it is recommended that databases be created and configured using the Enterprise Manager tools that are provided with the database software. This provides far greater control and flexibility over the configuration and administration of your databases.

Detaching a Database

Detaching a database involves the removal of all Agile Business Suite related tables and constructs from the specified database.

To detach a database using the Administration tool, right-click the required database node and select **All Tasks**, then **Detach From Runtime**.

This process does not delete the database.

Deleting a Database

The Administration tool can only be used to delete databases that were created using the Administration tool. Databases created using the database software must be deleted with the Enterprise Manager tools of the database software.

To delete a database using the Administration tool, right-click the required database node and select **Delete** from the context-menu.

When deleting a database, the database is checked to ensure there are no resident applications. If applications are still present, the database cannot be deleted. If there are no applications, but tables still exist, the database is detached and then deleted.

Section 8
Runtime for ClearPath MCP Installation and Configuration

This section describes how to install the Agile Business Suite Client Environment.

Notations

Where specific operating command strings are given, italics are used to delimit metatokens or variables. Enter an actual value in place of these variables as instructed. Square brackets delimit optional values.

Pre-Installation Requirements

Products and Terminology

This subsection gives a summary of the main Agile Business Suite Software products.

This subsection lists important terminology. Read this subsection carefully to help you understand how the instructions in this document relate to your particular type of software.

Runtime

Runtime is the term used for the programs and utilities needed to run deployed applications.

Deployed applications, Reports, and Networks cannot run on your host equipment until Runtime is installed.

Transferring an Application

Runtime Transfer – The Runtime Transfer utility enables built applications to be transferred to and from other MCP environments.

Configure – The Configure utility is used to install and configure an application from a magnetic tape or a directory of files produced on a different host.

Considerations

When transferring an application built under release 7.0 to another MCP based host, you must also use Runtime from release 7.0 on the target host.

Refer to the *Agile Business Suite Runtime for ClearPath MCP Administration Guide* for more information on transferring applications.

Required System Software Requirements

This subsection lists the required and the optional software for Agile Business Suite 7.0 Runtime for ClearPath MCP operations. Install the software according to the instructions included in the documentation for each item.

Caution

Using system software facilities to manipulate message content outside of functionality (for example, COMS PIs) is done at your own risk.

General Software Requirements

Agile Business Suite 7.0 Runtime for ClearPath MCP supports System Software Release 58.1 and 59.1 , including:

- COBOL85 (Note that COBOL74 cannot be used.)
- DMS II and DMSII XE

DMSII XE requires Extended Edition. If you are using Extended Edition features, you must have a license for Extended Edition.

- DMS/INQUIRY (optional)
- ERGO (optional)
- SYSTEM/CANDE
- SYSTEM/BINDER
- COMS
- DMALGOL
- Multi Lingual System (MLS)
- NEWP compiler

To interface with the ADDS Dictionary, the ADDS software must be installed.

MCP Releases Supported in this Release

Release	Qualification EPSILON (LEVEL5)	Qualification ETA (LEVEL6)	ALGOL IC Level for DUMPINFO Compatibility
MCP 20(SSR 62.0)	Supported	Qualified	MCP 62 [62.080.000]
MCP 19 (SSR 60.0)	Supported	Qualified	ALGOL-060.0A.10
MCP 18 (SSR 59.1)	Supported	Qualified	ALGOL-059.1A.3
MCP 17 (SSR 58.1)	Supported	**Not Supported**	ALGOL-058.1A.12

Although this release supports MCP 17, it is recommended that you install MCP 18 to be able to use all features.

These features require MCP 18 (SSR 59.1):

- ETA package
- Data Encryption

MCP Runtime Compatibility Matrix

Use this matrix to select an installation package for MCP Runtime.

AB Suite MCP Runtime Package	MCP Architecture ETA COMPILERTARGET LEVEL5	MCP Architecture ETA COMPILERTARGET LEVEL6
EPSILON LEVEL5 code files	Compatible (MCP 19, 20)	Compatible (MCP 19, 20)
ETA LEVEL6 code files	Incompatible	Compatible (MCP 19, 20)

Note: *Check the setting of the COMPILERTARGET option on your host. If it is set to LEVEL5, do not use the ETA package.*

Caution

Although the ETA package has undergone full engineering testing, it is highly recommended to perform a complete regression test before using the ETA LEVEL6 package in production.

AB Suite MCP Runtime will continue to ship two runtime packages until Unisys discontinues support for LEVEL5 code files.

Caution

For those who use Runtime Transfer, be aware that the LEVEL6 code files are incompatible with the EPSILON architecture. If your production machine has the EPSILON architecture, do not build the source system, for the transfer, with the ETA package. The LEVEL6 code files that are transferred to the machine with the EPSILON architecture does not run.

Minimum Software IC Levels for MCP 18

Software	IC Level
MCP	MCP-059.1A.10
COBOL85	COBOL85-059.1A.3
ALGOL	ALGOL-059.1A.3
BINDER	BINDER-059.1A.2
DMSII	DMSII-059.1A.10

Minimum Software IC Levels for MCP 19 (SSR 60.0)

Software	IC Level
MCP	MCP-060.0A.21
COBOL85	COBOL-060.0A.9
ALGOL	ALGOL-060.0A.10
BINDER	BINDER-060.0A.3
DMSII	DMSII-060.0A.14
OLEDB	OLEDB-060.0A.1

Minimum Software IC Levels for MCP 20 (SSR 62.0)

Software	IC Level
MCP	MCP-062.0A.12
COBOL85	COBOL85-062.0A.4
ALGOL	MCP 62 [62.080.000]

Software	IC Level
BINDER	MCP 62 [62.080.000]
DMSII	DMSII-062.0A.4

Software	IC Level
MCP	MCP 63 [63.080.000]
COBOL85	MCP 63 [63.080.000]
ALGOL	MCP 63 [63.080.000]
BINDER	MCP 63 [63.080.000]
DMSII	MCP 63 [63.080.000]
FTP	MCP 63 [63.080.000]

Network Software Requirements

To support cross-host transactions, networking capability is required.

If you do not require cross-host communications, then local port capability is provided by LPPSUPPORT.

If you require cross-host communications, BNA V2, TCP, or OSI are required.

If you require interhost system services (for example, file transfers), you must also install Distributed System Services (DSS). You need to install this if you are going to use the Agile Business Suite Builder or the Remote Subroutine Server.

If you require Agile Business Suite Debugger to call subroutines on the host, you must install the Remote Subroutine Server (also known as LRSS) in addition to DSS. Refer to Installing and Configuring Remote Subroutine Server.

If you intend to use Enterprise Output Manager for printing Reports, then you need to install and configure the Enterprise Output Manager software for the MCP based hosts. This enables the MCP based applications to direct print output to the Enterprise Output Manager PC Server when the default output device is set to DP. Refer to the *Enterprise Output Manager* documentation for more information on installing and configuring Enterprise Output Manager on the MCP based host.

Other Software Release Compatibility

The following software release compatibility is required:

- Developer

  Agile Business Suite Release 7.0 supports Case Interchange File (LCIF) interchange with Enterprise Application Developer 3.3, and Agile Business Suite 2.0, 3.0, 4.0, 5.0, 6.1, and 7.0.

Minimum Hardware Requirements

The following hardware is necessary to use Agile Business Suite 7.0 ClearPath MCP based software:

- MCP based mainframe, with a minimum of 50 Megabytes of memory. Agile Business Suite 7.0 is compatible with all MCP based platforms that are currently supported by Unisys.
- Unisys T27 emulators and WebEnabler

  Refer to Configuring Terminal Devices for Runtime for ClearPath MCP for more information.
- Line printer (optional).
- Disk space. Sufficient to support the minimum disk requirements shown in the following table (based on release 7.0 configured with default settings and using a secondary audit file).

Files	Sectors	Description
NGEN28/=	217000	Skeleton files and general utilities common to all applications.
Other Files	18000	Other database files and COMS Configuration File
Total	1061000	

In addition, the following table shows the requirements needed on DISK. These files are shared by all end-users on the host.

Files	Sectors	Description
NGEN28/=	32000	Shared files and programs
Others	250	EXAMINER and LINCXSUPPORT files

As disk and memory requirements vary, contact your Unisys representative for planning assistance.

Setting Up the Host

Before you install and configure your software, you should perform the following tasks:

- Set the Host Name for your system.
- Ensure SYSTEM/BINDER, SYSTEM/DASDL, SYSTEM/DMALGOL, and SYSTEM/COBOL85 are accessible for your usercode.
- Ensure that the SSR level of the compilers and DMSII software that are installed on your machine for AB Suite builds is supported by AB Suite MCP Runtime.
- MCP 18 (SSR 59.1) must be installed to use the ETA package with LEVEL6 code files.

  The ETA package does not support MCP 17 (SSR 58.1).
- If configuring with a Dictionary or Work pack that is the alternate family for the usercode under which you run the configure option. Then, before the configure job is run, change the usercode family to:

  ```
  DISK = alternate ONLY.
  ```

  This ensures the appropriate files are copied to the correct pack.
- Ensure that an SL command has been performed on the library KEYEDIOIISUPPORT on your system. Setting the KEYEDIOII is recommended but not required.

Configuring Terminal Devices for Runtime for ClearPath MCP

COMS Station Definitions

COMS station definitions, as used by Agile Business Suite Runtime for ClearPath MCP, make use of fields within COMS Installation Data entities. The use of these fields is shown in the following table.

Field	Usage	Description
Integer1	Station type	0 = ET/TD/T27
		1 = ET/TD/T27
		4 = NOFORM interface
Integer2	Access level	0 = Standard
		1 = ODT
		2 = Controller
Integer3	Privilege level	1 – 15
String1	Associated printer	First 17 characters
	Model	Characters 18 – 34
String2	Default language	Language name, up to 15 characters

Notes:

- *If Integer1 is equal to 0 for a station, when Agile Business Suite receives a BYE from that station, a ?CLOSE request is sent from the station.*
- *When Integer1 is equal to 1, Agile Business Suite performs a programmatic CLOSE of the window.*
- *If the Integer3 value for your station is less than the user privilege level for an Ispec (as set on the Component/Event Choices screen), you will see the error message:*

  ```
  Insufficient privilege for ispec
  ```

  when you try to access the Ispec from your station.
- *Printers must have IDs in order to define Models.*

If you have external applications that use Installation Data entities, and these conflict with the way in which Agile Business Suite Runtime for ClearPath MCP uses these entities, you should define your non-external entities as secondary Installation Data, and then associate this secondary Installation Data with the primary.

Configuration Settings for Terminals Qualified for Agile Business Suite Runtime for ClearPath MCP

Refer to terminal device reference material for more information on configuration. The required register settings for terminal devices are given in the following subsections (by device type). The convention *XX XX* represents a unique terminal address (in hexadecimal).

General Requirements

When defining terminal devices:

- Do not use braces as alternate forms characters.
- Agile Business Suite Runtime for ClearPath MCP requires terminals capable of displaying a 72-character status line.
- Where applicable, configure your terminal so that carriage returns are not visible.

TD 830 and TD 830J (9600 BPS TDI)

Location	Hex Settings
0080	OA FB 01 00 17 4F 1F 1E 10 XX XX 04 09 00 04 04
0090	00 2F 4F 17 4F FF 00 4F 17 40 00 08 03 50 0F FF
00A0	04

MT 983/5 (9600 BPS TDI), level 3 firmware

Location	Hex Settings
0080	OA A1 01 03 17 4F 1F 1E 10 XX XX 47 08 01 47 41
0090	00 2F 4F 17 0F 00 00 4F 17 00 00 08 00 00 07 80
00A0	04

SR-100 and SR-110

Datacomm	Setting
Databits	7
Parity	E
Syn	N
60 Hz	Y
2 Stop Bits	N
ACK Level	0051
XMIT #s	N

Edit	Setting
Stay in receive	Y
Forms XMIT to cursor	Y
SOH Exits Forms	Y
SOH Clears Page	N
Auto Page Adv Enable	N
DC1=Stay In RCV	Y
DC2=Toggle Forms	Y
Dcom LF->CR	N
Dcom CR->LF	Y
ETX Plant From Dcom	N
CR Plant From Kbd	N

ET 1100 and T 27 Terminal/Emulator Configuration Menu

Option	Value
LINE/Page	24
CHAR/Page	80
LINE/SCREEN	24

To print on AP 1312 or AP 1314 terminal printers from an ET 1100, the PRINT GROUP options must be set to the default values, with the following exceptions:

Option	Value
BITS/CHAR	7
AUX INPUT	D
BUSY (I/O)	1
SPECIFY KEY	A

In addition, the following values must be set.

Option	Value Required
SCREEN	17280 (max)
ALT FORM DELIMITERS OPEN (US)	1F
CLOSE (RS)	1E
PRINT AUX	2-character address of background printer
PRINTER DCOM	2048 (min)
PRINT BPS	Must be set as relevant for particular printer

TC 4000J

On switch SW734, bits 4 through 8 (inclusive) must be closed.

Installing and Configuring Runtime for ClearPath MCP

Preparing for Installation

Before commencing installation, read Pre-Installation Requirements and Installation Checklist.

In addition, it is important that you read your Agile Business Suite 7.0 Runtime for ClearPath MCP Software Release Announcement (SRA) before commencing installation. You must note carefully any listed conditions or restrictions that might apply to you.

Installation Checklist

Use this checklist when considering the issues and the steps you must take before and after you install your software. (Unless specifically stated otherwise, references in the table are to topics later in this section).

If you are already a user, you only need to confirm that your current pre-installation setup is correct before migrating to this release.

Step	Action	References
1	Review the Agile Business Suite terminology and product range	Products and Terminology
2	Verify that you have the correct release media	Required System Software Requirements
3	Verify that you have the necessary hardware	Minimum Hardware Requirements
4	Verify that you have the necessary software	Required System Software Requirements
5	Check your host setup.	Setting Up the Host
6	Ensure that your terminal device configurations are appropriate for Agile Business Suite.	Configuring Terminal Devices for Runtime for ClearPath MCP
7	If you are already a user, consider any relevant conversion issues.	Migration Procedure
8	Installing the software.	Installing the MCP Runtime Software
9	Verify that you have the appropriate COMS configuration for your site requirements.	Configuring COMS for Applications

General Notes About Installation

Before initiating the installation process, you should be aware of the points outlined in the following subsections.

Setting Up Tasklimits

When configuring software, the Configuration WFL job might terminate because the number of spooled tasks exceeds the Tasklimit for the queue. You can avoid this happening by submitting the Configuration WFL to a queue that does not have the Tasklimit attribute set. The maximum value of the Tasklimit is 31.

Required Supplementary Files

The following files are copied to DISK (or the alternate family pack), provided that the version being installed is higher than the version currently in place. (If it is not, the files are not copied from the Dictionary specified during installation, and a message is displayed.)

```
*NGEN28/1/LIBRARY
*NGEN28/1/LTEACH
*NGEN28/MLSLIBRARY
*NGEN28/1/HUBROUTER (copied to same pack as COMS)
*NGEN28/UTILITY/LINCFORM
*NGEN28/GLI
*NGEN28/OFF
*NGEN28/LVU
*NGEN28/RIP
*NGEN28SYS/CODES
*EXAMINER/LIBRARY
*SYSTEM/LINCXSUPPORT
```

Using a Privileged Usercode for Installation

The usercode from which the RUNTIME job is started must be privileged. If the RUNTIME job is started from a non-privileged usercode, any SLs for libraries released with this cut must be done manually from MARC under a privileged usercode.

If your machine has Security Administrator status enforced (by enabling the SECADMIN option), the usercode from which the RUNTIME job is started must have SECADMIN privileges. If the usercode does not have SECADMIN privileges, any SLs for libraries released with this cut must be done manually. Therefore, you must decide which usercode to use before you begin the installation.

Runtime Transfer Considerations

If you are installing AB Suite on environments used in Runtime Transfers, you must install the release from the same installation package in both the source and the target runtime environments.

Installing multiple Runtimes on the same MCP host

If you are installing multiple Runtimes on the same MCP host, each installation must be installed under separate usercodes with different APPL_BLD identities and unique port numbers. Each installation of Application Builder (APPL_BLD_) requires its own runtime environment. More information on installing APPL_BLD can be found in the installation instructions.

Unwrapping the GCA container for a First-Time Installation

If this is the first time that the runtime is being installed in the designated runtime usercode and you have not installed the GCA release already, you must make the GCA files available for installation now.

The GCA release media contains two packages.

1. EPSILON package with LEVEL5 code files.
2. ETA package with LEVEL6 code files.

See Required System Software Requirements to view the MCP Runtime Compatibility Matrix. The MCP Runtime Compatibility matrix helps you to choose the package that is compatible with your MCP host architecture and MCP release. When you choose a package from the IC release, ensure that it is compatible too.

Follow these steps to unwrap the files from the GCA release:

1. Copy the GCA release to Windows and mount the ISO image file.
2. Map a network drive to your privileged usercode on the MCP host.
3. Copy the GCA container file from the ISO image to the MCP host. Select the container with the package you want to install.
   - EPSILON: GCA-70-1000-02.CON
   - ETA: ETA-GCA-70-1000-02.CON
4. Disconnect the network drive.
5. From CANDE, unwrap the files to the transfer pack:

   EPSILON

   ```
   WFL UNWRAP *= OUTOF "GCA-70-1000-02.CON"
   To <Transfer Pack>(RESTRICTED = FALSE)
   ```

   ETA

   ```
   WFL UNWRAP *= OUTOF "ETA-GCA-70-1000-02.CON"
   To <Transfer Pack>(RESTRICTED = FALSE)
   ```

Copying the Runtime Install Job from the Release Media

The release media contains two packages.

1. EPSILON package with Level5 code files.
2. ETA package with LEVEL6 code files

See Required System Software Requirements to view the MCP Runtime Compatibility Matrix. The MCP Runtime Compatibility Matrix helps you to choose a package that is compatible with your MCP host architecture and MCP release.

To copy the MCP Runtime install job from the release media, perform the following:

1. Obtain the release medis, copy the IC release to Windows.
2. Map a network drive to your privileged usercode on the MCP host.
3. Copy the ICcontainer file from the ISO image file to the MCP host. Select the container with the package you want to install.

   EPSILON: IC-70-<IC number>.CON

   ETA: ETA-IC-70-<IC number>.CON

4. Disconnect the network drive.

5. From CANDE, log in using the privileged usercode and unwrap the container file:

   EPSILON

   ```
   WFL UNWRAP *= OUTOF "IC-70-<IC number>.CON"
     TO <Transfer pack>(RESTRICTED=FALSE)
   ```

   ETA

   ```
   WFL UNWRAP *= OUTOF "ETA-IC-70-<IC number>.CON"
     TO <Transfer pack>(RESTRICTED=FALSE)
   ```

6. Download the IC install WFL:

   EPSILON

   ```
   COPY (TRANSFER)IC/70/<IC number>/NGEN28/WFL/RUNTIME
   AS NGEN28/WFL/RUNTIME
   FROM <Transfer pack>(PACK)
   ```

   ETA

   ```
   COPY (TRANSFER)ETA/IC/70/<IC number>/NGEN28/WFL/RUNTIME
   AS NGEN28/WFL/RUNTIME
   FROM <Transfer pack>(PACK)
   ```

Installing the MCP Runtime Software

To install the MCP Runtime Software, perform the following:

1. Logon to your privileged usercode.

2. Start the Runtime WFL, by entering:

   ```
     START NGEN28/WFL/RUNTIME
     ("usercode","pack","aliaspack",
   FALSE, GCA media parameter  )
   ```

   The *usercode* value is the usercode to which the Runtime is installed, which might be an asterisk (*).

   The *pack* value is the family name of the pack to which the Runtime is installed, which might be *DISK* or *altpack*.

   The *aliaspack* value is the pack for your station alias file. Refer to the *Agile Business Suite Runtime for ClearPath MCP Administration Guide* for more information on station aliases.

   GCA media parameter = "MD=*MediaDirectory* MN=*MediaName* N=*Cut#*"

   MediaDirectory is the directory containing the installation files:

   EPSILON

   (TRANSFER)GCA

   ETA

   (TRANSFER)ETA/GCA

   MediaName is the name of the pack on which the installation files are located.

<Transfer pack>

Cut# is the cut number for the release.

1000-<nn>

For example:

"MD=(TRANSFER)ETA/GCA MN=TFRPACK N=1000-02"

Notes:

- *The usercode from which the RUNTIME job is started must be privileged.*

  If the RUNTIME job is started from a non-privileged usercode, any SLs for libraries released with this cut must be done manually from MARC under a privileged usercode.

- *If your machine has Security Administrator status enforced (by enabling the SECADMIN option), the usercode from which the RUNTIME job is started must have SECADMIN privileges.*

  If the usercode does not have SECADMIN privileges, any SLs for libraries released with this cut must be done manually.

3. License Agreement – Before the installation begins, you will be asked to accept the license agreement. The installation job is suspended twice to allow you to read the license information. The terms of the license agreement might be found in the instruction blocks. Enter ?<mix> IB nn from MARC to view each instruction block. Enter ?<mix>OK to accept the license agreement and install Agile Business Suite 7.0 for the MCP Operating System.

4. During the installation, you will be prompted:

   ```
   ** DO YOU WISH TO OVERWRITE EXISTING LIBRARIES (HUBROUTER, RATL, ETC.) WITH THE
   LIBRARIES IN THIS RELEASE?
   AX YES TO OVERWRITE OR AX NO TO INSTALL/RETAIN LATEST VERSION **
   ```

   This allows you to overwrite existing libraries, even if their release level is higher than the GCA release.

   Respond with AX YES to overwrite existing libraries.

   Respond with AX NO to allow the installation job to use release checking and only install the new libraries if they have a higher release level than the existing libraries.

5. During the installation, you will be prompted to confirm the version of AB Suite 7.0 MCP Runtime that is being installed.

   Respond with OK to confirm.

   DS the job to terminate the installation.

6. During the installation, you will be prompted for the SSR level of the LOGIC and DUMPINFO files to be installed. The SSR level must match that of the DMALGOL compiler currently installed on your system. You will be prompted to respond to the waiting entry with one of the following:

   EPSILON

   581, 591, YES

   ETA

591, YES

The meanings of these are:

Response	Meaning	Compatible with DMALGOL compiler
581	Install 581 LOGIC and DUMPINFO files	IC ALGOL-58.1A.12
591	Install 591 LOGIC and DUMPINFO files	IC ALGOL-59.1A.3
YES	Install the LOGIC files for the corresponding, supported MCP SSR	

If you respond with YES and your MCP release level is not supported, you will be prompted to enter the SSR level of a DMALGOL compiler that is installed on your system and is supported.

If the SSR level you have selected is not the SSR level of the default compilers, you are advised to modify the TASKSTRING attribute of NGEN28SYS/BLD with the location of the compilers after the IC installation is complete.

```
WFL MODIFY (<Runtime Usercode>)NGEN28SYS/BLD ON <Runtime Pack>;
TASKSTRING= "[Tparam,]<compiler list>";
```

Where <Tparam> is T=5.

Include this if you are installing the EPSILON package on a host with the ETA architecture.

Where <compiler list> is

```
C=<COBOL85 compiler>, D=<DMALGOL compiler>, B=<BINDER>
```

For example,

```
WFL MODIFY (RTUSER)NGEN28SYS/BLD ON RTPACK;
TASKSTRING= "T=5, C=*COBOL85/591, D=*DMALGOL/591, B=*BINDER/591";
```

or

```
WFL MODIFY (RTUSER)NGEN28SYS/BLD ON RTPACK;
TASKSTRING= "C=(MYUSER)COBOL85/600 ON MYPACK,
D=(MYUSER)DMALGOL/591 ON MYPACK, B=(MYUSER)BINDER/591 ON MYPACK";
```

7. During the installation, you will be prompted for the SSR level of the SMU, DMU and CFG codefiles to be installed. The SSR level must match that of the DMSII level of the application databases that are built by the runtime being upgraded. You will be asked to respond to the waiting entry with one of the following:

   EPSILON

   581, 591, YES

   ETA

   591, YES

   The meanings of these are:

Response	Meaning
581	Install 581 SMU, TRANSFER, DMU, and CFG files
591	Install 591 SMU, TRANSFER, DMU, and CFG files
YES	Install SMU, TRANSFER, DMU, and CFG files for the corresponding supported MCP SSR

If you respond with YES and your MCP release level is not supported, you will be asked to enter a supported level of DMSII that is installed your machine.

If the systems that are deployed by this runtime environment use DMSII software located under a usercode and on a pack, as specified by DMSII Usercode and DMSII pack segment configuration properties in the configuration of the segment, the SSR level selected for SMU, DMU, and CFG should correspond to the SSR level of the DMSII software.

If there are AB Suite application databases of different DMSII release levels, some use 58.1 and some use 59.1, for example, it is strongly recommended that separate runtime environments should be created to handle the different levels. Designate one runtime for SSR 58.1 and one for SSR 59.1.

8. During the installation, you might be prompted to acknowledge that an updated version of MLSLIBRARY has been installed. Respond to the waiting entry with **OK**. If you use a language other than ENGLISH, check for untranslated messages in the file

   NGEN28/MLSLIBRARY/UNTRANSLATED.

9. During the installation, you will be asked whether you wish to install Application Builder.

   You will be asked “DO WISH TO INSTALL APPL_BLD? AX YES/NO”. You have the choice of installing the default Application Builder or a clone. If you wish to install either, respond with ?<mix#> AX YES, otherwise respond with ?<mix#>AX NO.

   If you respond with YES, you will then be asked “DO YOU WISH TO INSTALL CUSTOM OR DEFAULT APPL_BLD? AX C FOR CUSTOM OR D FOR DEFAULT”.

   Installing Application Builder with Default Identity

   Respond with ?<mix#>AX D if you wish to install the default Application Builder. This creates/modifies APPL_BLD_70.

   Installing Application Builder with Custom Identity

   Note: *Each cloned Application Builder requires its own runtime environment. Each time you clone an Application Builder with a new identity, you need to install a new environment for it.*

   To install Application Builder with Custom identity, you need the following details:

<identity>	An identifier for the MCP Builder Server (limit of 6 characters). For example, 70A for APPL_BLD_70A. By default, the identity is 70 (for 7.0). You might choose an identity of up to six alphanumeric characters.
<port number>	A port file number from which to connect (this must be a unique number). By default, the port number is 8800. Do not use this number.

Respond with ?<mix#>AX C, if you wish to install a custom version of MCP Builder Server. Next, a message appears,

"PLEASE ENTER IDENTITY AND PORT NUMBER TO BE USED WITH CUSTOM APPL_BLD".

You are then prompted to enter the identity for the custom APPL_BLD:

"AX IDENTITY TO BE USED WITH CUSTOM APPL_BLD (MAX 6 CHARS)"

Respond with ?<mix#>AX <identity>

Next, you are prompted to enter the port number for the custom APPL_BLD:

"AX PORT NUMBER TO BE USED WITH CUSTOM APPL_BLD"

Respond with ?<mix#>AX <port number>

Note: *Nulls are not accepted. If you enter nulls for either, you are required to enter the identity and port number again.*

After entering the identity and port number, you are asked to confirm what you entered:

"FOR CUSTOM APPL_BLD YOU ENTERED: ID=<identity>, PORT=<port>,

IS THIS CORRECT? AX YES OR NO"

If it is correct, respond with ?<mix#>AX YES, otherwise respond with ?<mix#>AX NO and enter them again.

After Installing Application Builder

Check for waiting entries in the mix. You might need to respond to a request to initialize the APPL_BLD files. Respond to the initialization request with one of the following:

- Y to initialize a new APPL_BLD files.
- N to terminate APPL_BLD.
- C <file title> to convert an existing CPA file.

10. During the installation, you will be asked whether you wish to install RATL, LRSS, and TPTOMARC. If you wish to install either of them, respond with ?<mix>AX YES, otherwise respond with ?<mix>AX NO.

11. If you have installed an update to RATL during the installation, you must disable and enable RATLPCM to activate the new server.

```
NA CCF DISABLE PCM RATLPCM
NA CCF ENABLE PCM RATLPCM
```

12. Set up the required Support Libraries (SLs).

    If you did not start the Runtime install job with adequate privileges for the SLs to be done automatically, set up the required Support Libraries (SLs) now.

    If your host has Security Administrator (SECADMIN) status enforced, sign on to MARC with a SECADMIN status usercode. (Only a user/task/job with SECADMIN status might issue SL commands when SECADMIN status is enforced.)

    From MARC, enter:

    ```
    SL NGEN28SERVICES = *NGEN28/1/LIBRARY ON altpack
    SL EXAMINERLIB = *EXAMINER/LIBRARY ON altpack
    ```

    The *altpack* gives the alternate pack for the family of the usercode under which you are running Runtime. For example, your usercode family might be specified as follows:

    ```
    DISK = INTPACK OTHERWISE SYSPACK
    ```

    If so, enter *SYSPACK* as your *altpack* value.

    Configuration of Runtime is complete. For your next steps, refer to Configuring COMS for Applications.

Data Masking

There are two ways to specify masking if secure fields in the LINCLOG –

1. Using the **LOGLIBSECURITY** utility.
2. Using the **EnableMaskDefinition** property of an attribute then specifying a mask with the **MaskDefinition** property.

To use option 1, set the DEFAULTMASKING Boolean in NGEN28/WFL/GENERATE to FALSE

To use option 2, set the DEFAULTMASKING Boolean in NGEN28/WFL/GENERATE to TRUE.

UVMS: Setting up for Failover in a High Availability Environment

To prepare for failover, copy the GCA release to your MCP host and modify the constants in the LIB/INSTALL Parameters section of (<runtime usercode>)NGEN28/WFL/LIBS/INSTALL <runtime pack>.

1. Copy the GCA release to Windows and mount the ISO image file.
2. Copy the GCA container file from the ISO image to the MCP host. Select the container with the package you want to install.

   EPSILON: GCA-70-1000-nn.CON

   ETA: ETA-GCA-70-1000-nn.CON
3. From CANDE, unwrap the container file.

   EPSILON

```
WFL UNWRAP *= OUTOF "GCA-70-1000-nn.CON" TO <Transfer pack> (RESTRICTED=FALSE)
```

ETA

```
WFL UNWRAP *= OUTOF "ETA-GCA-70-1000-nn.CON" TO <Transfer pack> (RESTRICTED=FALSE)
```

4. Load down the LIB/INSTALL WFL:

   EPSILON

   ```
   COPY (TRANSFER)GCA/70/1000-nn/NGEN28/WFL/LIBS/INSTALL AS
   (<runtime usercode>)NGEN28/WFL/LIBS/INSTALL
   FROM <Transfer pack>(PACK) TO <Runtime pack>(PACK)
   ```

   ETA

   ```
   COPY (TRANSFER)ETA/GCA/70/1000-nn/NGEN28/WFL/LIBS/INSTALL
   (<runtime usercode>)NGEN28/WFL/LIBS/INSTALL
   FROM <Transfer pack>(PACK) TO <Runtime pack>(PACK)
   ```

   Open (<runtime usercode>)NGEN28/WFL/LIBS/INSTALL ON <runtime pack>.

5. Modify the constants under LIB/INSTALL Parameters:

   PRTUSERCODE = “<runtime usercode>”

   PRTPACK = “<runtime pack>”

   PICPREFIX = “(TRANSFER)GCA”

   PMEDIANAME = “<Transfer Pack>”

   PICNUMBER = “1000-nn”

   PAPPLBLDID = “70”

   PAPPLBLDPORT = “8800”

   PINSTALLTEACH = “YES”

   PINSTALLRATL = “NO”

   PINSTALLLRSS = “NO”

   PINSTALLTPTOMARC = “NO”

   Mandatory changes:

   PRTUSERCODE – MCP Runtime usercode

   PRTPACK – MCP Runtime pack

   PMEDIANAME – location of the GCA installation files

   Change the APPL_BLD PORT number if the runtime does not use the default

   APPL_BLD ID

   PAPPLBLDPORT

   Optional changes: set the ones to be installed to YES and set rest to NO.

   PINSTALLTEACH

   PINSTALLRATL

   PINSTALLLRSS

PINSTALLTPTOMARC

6. Save (<runtime usercode>)NGEN28/WFL/LIBS/INSTALL ON <runtime pack>.

Configuring COMS for Applications

The Configure Utility automatically loads the COMS Configuration file for your software into COMS. You might override this automatic load by supplying a user-coded library, as described later in this subsection.

This automatic load does not apply to the COMS Stations file for new or changed Networks. You must manually load the COMS Configuration for NOF if required.

Note: *The COMS UTILITY window must be configured to support multiple active users, as the Auto-load process takes up one user slot. If the Maximum Users value is exceeded, the automatic load fails.*

Inhibiting or Interrupting Automatic Loading

The Configure Utility calls an entry point in a user-supplied library, and passes the COMS Configuration file name as a parameter. The library can programmatically verify and/or modify the parameter to allow or disallow the automatic loading.

Library File

The library file must be accessible under the file search path for the usercode under which you configured Agile Business Suite. The file is titled:

```
*NGEN28/USERLIB
```

If the library file is not found, or the library linkage fails, automatic loading proceeds.

Entry Point

The entry-point is *COMSVERIFY*, defined as:

```
INTEGER PROCEDURE COMSVERIFY (COMS_LOAD_FILE_TITLE);
EBCDIC ARRAY COMS_LOAD_FILE_TITLE [0];
```

The COMS_Load_FILE_TITLE parameter contains the title of the COMS Configuration file to be loaded. This file might be changed or replaced by a privileged process.

Return Values

The COMSVERIFY procedure should return one of the following values:

- The value *1* if the file is to be loaded.
- The value *0* if the file is *not* to be loaded.

Example

The following ALGOL procedure inhibits the automatic load for a usercoded application whose COMS Configuration file name begins with *XX*. Non-user-coded applications have *COMS* after the first slash (/) character.

```
$SET LIST
BEGIN
INTEGER PROCEDURE COMSVERIFY (COMS_LOAD_FILE_TITLE);
EBCDIC ARRAY COMS_LOAD_FILE_TITLE [0];
BEGIN
% % Find out the system name:
% %
% % Take characters after the first slash (/):
% % - See if they start with "XX"
% % - If not, proceed with automatic load
% %
POINTER PA;
PA := COMS_LOAD_FILE_TITLE;
SCAN PA:PA UNTIL EQL "/";
% % Left pointing at the final "/"
PA := PA+1;
IF PA EQL "XX"
THEN
BEGIN
DISPLAY ("** COMS Autoload suppressed **");
COMSVERIFY := 0;
END
ELSE
COMSVERIFY := 1;
% %
END; % % of COMSVERIFY
% %
EXPORT COMSVERIFY;
FREEZE (TEMPORARY);
END.
```

COMS Configuration for the SwitchTo Command

The SwitchTo command requires a COMS processing item such as TPTOMARC, to be installed for the MARCINPUT agenda in the COMS configuration data.

The TPTOMARC processing item is provided on your release media in the sample file:

```
NGEN28/SAMPLE/TPTOMARC/PROCITEM
```

Refer to the example of the TPTOMARC processing item in your COMS documentation for more information.

Installing and Configuring the Remote Access Server (RAS)

Introduction to Remote Access Server

The Remote Access servers can be used by Component Enabler to access applications.

The server-side deployment consists of a number of platform-specific Remote Access servers that handle communications between clients and applications. Clients and servers communicate, using RATL protocol running on TCP/IP. This protocol is a simple wrapping of a standardized and extended set of NOF messages that provide all the functionality needed to support GUI forms.

Clients establish normal sessions with applications through the Remote Access servers using a TCP/IP connection. These servers perform a number of checks, such as authenticating users and verifying the application exists, before granting the client access. The servers then receive transaction requests from client programs over a TCP/IP connection and pass them to the application. Transaction responses from applications are passed back to the clients over the same TCP/IP connection. Remote Access servers can also pass back asynchronous messages, such as messages from Reports, to a client application.

Remote Access servers can also use the Microsoft Message Queue (MSMQ) server for connections instead of TCP/IP connections.

The Remote Access servers are designed to offer connectivity, throughput, and transit times comparable to terminal access to the applications on the same host applications. Each client application runs independently of all other clients, with its own connection back to the application server. There are no points of single threading or possible congestion in the transaction path to add overheads or reduce performance.

Installing Remote Access Server

Codefile

The codefile is automatically installed to the CCF system pack.

CCF params file

- Obtain the sample CCF params file for the Remote Access Server, named:

  ```
  (<ABSUITE usercode>)NGEN28/SAMPLE/CCF/
  PARAMS/RATL ON <ABSUITE dictionary>
  ```

- Enter the Remote Access Entities required. Refer to CCF Configuration in Installing and Configuring Remote Subroutine Serverfor more information on configuring entities.
- Insert the definitions into the current copy of the CCF params file,

  ```
  SYSTEM/CCF/PARAMS ON <CCF PACK>
  ```

  Note: *For A-Series Systems the CCF params file might not be present. Create this file using the sample provided:*

  ```
  (<ABSUITE usercode>)NGEN28/SAMPLE/
  CCF/PARAMS ON <ABSUITE dictionary pack>
  ```

COMS

Register the entities to COMS via the Utility window with the following file:

```
(<ABSUITE usercode>)NGEN28/SAMPLE/COMS/CONFIG/RATL ON <ABSUITE dictionary pack>
```

For Big Buffers, set the Maximum Message Text size for Global Activity to 65000.

CCF Configuration

Use the CCF components to configure the server entities as follows:

CCF Component	Entity
Router	PCM
CUCI	Device and Service
TCPIP	Port
RATL	Service, View, Language, MQserver, MQclient, and MQrequest

Router

Identify the server as a PCM to the router and enable it, using the following syntax:

```
Add PCM <name>
 codefile = <filepath>
Enable PCM <name>
```

Attributes	Description
<name>	Identifies a valid server name.
<file path>	Specifies the codefile path.

Example:

```
Add PCM <name>
 codefile = <filepath>
Enable PCM <name>
```

CUCI

As part of the CCF configuration you must configure a:

- Connection Device
- Connection Service

Connection Device

Configure a device to the CUCI PCM to associate device connection attributes with each dialog. Attributes are assigned using the following syntax:

```
Add Device <device name>
 acvt = <VTname>,
 ccenable = <boolean>,
 controlcapable = <boolean>,
 dynamic = <boolean>,
 marccapable = <boolean>,
 maxinput = <number>,
 maxoutput = <number>,
 messages = <category>,
 securitycatlist = <name>,
 ndlheader = <boolean>,
 screen = <boolean>,
 usage = <category>
```

Attributes	Description
<device name>	Defines a unique device name.
acvt	Specifies an Application Controller Virtual Terminal. This is the virtual terminal COMS expects the client to be using on input. This attribute is optional. <VT name> must be set to either Transparent or Default.
ccenable	Indicates if control character processing is enabled. This attribute is optional. This attribute can only be set to False.
controlcapable	Indicates if control commands can be entered or not. This attribute is optional. This attribute can only be set to False.
dynamic	Indicates if the connection is to be kept by COMS when the connection terminates. This attribute is optional.
marccapable	Indicates if the connection can handle screen output from MARC. This attribute must be set to True if you are to use the RATL Services attribute **MARCOpenText**.
maxinput	Specifies the maximum number of bytes in an input message. For Big Buffer Ispecs, this must be set to 45300 (65000 for Big Buffer Ispecs not using POF). <number> must be a minimum of 2500.
maxoutput	Specifies the maximum number of bytes in an output message. For Big Buffer Ispecs, this must be set to 45300 (65000 for Big Buffer Ispecs not using POF). <number> must be a minimum of 2500.
messages	Determines whether application messages are displayed at the client. <category> must be set to None.

Attributes	Description
securitycatlist	Specifies a COMS Security Category List configuration entity that is defined in COMS. When set, the value of this attribute is the default value used when connecting to COMS. It can be overridden by the service attributes of NOFidentity. This attribute is optional.
ndlheader	This attribute is optional. This attribute can only be set to False.
screen	Indicates whether the client is a screen device. This attribute is optional. This attribute can only be set to False.
usage	Identifies whether the client can receive input messages, send output messages, or both. <category> must be set to one of In, Out, or IO. The recommended value is IO, so that the client can both send and receive messages.

Example

```
Add Device RATLweb
 acvt = transparent,
 ccenable = false,
 controlcapable = false,
 dynamic = true,
 marccapable = false,
 maxinput = 10000,
 maxoutput = 10000,
 messages = none,
 securitycatlist = SCL_NOF,
 ndlheader = false,
 screen = false,
 usage = IO
```

Connection Service

Configure a service to the CUCI PCM to associate device connection attributes and to identify the connection path for each dialog. Attributes can be assigned using the following syntax:

```
Add Service RATLon
 closeaction = <number>,
 device = <name>,
 logoffdisconnect = <boolean>,
  dynamic = <boolean>
Enable Service RATLon
```

Attribute	Description
closeaction	The SYSTEM/COMS Close Action as defined on the SYSTEM/COMS Usercode menu. The close action is also defined on the Station menu of the COMS Utility. You must enter a value in the range 1 to 4. ***Note:*** *If the dynamic attribute is set to True, the action is that of the DefaultStation definition in COMS.*
device	You must provide a CUCI Device Name. This does not need to be a valid SYSTEM/COMS Device name.
dynamic	Indicates if the connection is to be kept by COMS. This attribute is optional. Allowed values are: • True, the connection is not kept by COMS • False, the connection is kept by COMS.
logoffdisconnect	Indicates whether the session is automatically logged off when the connection is terminated. This attribute must be set to True.

Example

```
Add Service RATLon
 closeaction = 3,
 device = ratlweb,
 logoffdisconnect = true
Enable Service RATLon
```

Note: *For services, the **service name** associated with the declared service is the name of the next service in the connection path*

TCPIP Port

Define a port to the TCPIP PCM to associate port attributes for the dialogs. Attributes can be assigned using the following syntax:

```
Add Port <port name>
 stationname = <name>,
 checkinterval = <number>,
 device = <name>,
 framing = <category>,
 maxoffer = <number>,
 maxoutput = <number>,
 service = <name>,
 socket = <number>,
 transport = <category>,
 windowsize = <number>
Enable Port <port name>
```

Attribute	Description
<port name>	Specifies a unique port name. <port name> must correspond with an identified service.
stationname	Specifies a unique station name. Refer to Using StationName.
checkinterval	Specifies the period of inactivity before keep alive packets are sent. <number> is specified in seconds, and must be in the range 0 through 1440.
device	Specifies the name of a device to be used for all subport connections that are passed to the CUCI PCM. <name> must be a previously configured device.
framing	Specifies the type of message delineation to be used. Message delineation indicates where a message starts and ends. <category> must be set to Standard.
maxoffer	Specifies the number of subports to be offered (made available for connection) at any time. <number> must be in the range 0 through 31.
maxoutput	Specifies the maximum number of bytes in an output message. For Big Buffer Ispecs, this must be set to 45300 (65000 for Big Buffer ispecs not using POF). <number> must be in the range 128 through 65535.
service	Specifies the name of a service to be used for inbound subport connections. This is the next service in the connection path. <name> defaults to <port name>.
socket	Specifies the socket number used by the client to connect to the port file. <number> should be set to the recommended value of 2449, unless a non-standard port configuration exists.
transport	Identifies the transport to be used. <category> must be set to TCPIP, or it defaults to null.
windowsize	Specifies the maximum number of bytes that can be queued, on input, per dialog before more is received. For Big Buffer Ispecs, this must be set to 45300.

Example

```
Add Port RATL
 stationname = actlinc/#,
 checkinterval = 5,
 device = ratlweb,
 framing = standard,
 maxoffer = 1,
 maxoutput = 10000,
     service = ratl,
     socket = 2449,
     transport = tcpip,
     maxoffer = 500
    Enable Port RATL
```

Using StationName

This attribute names a connection to COMS. It provides a flexible format from which station names can be generated.

Note: *Refer to <tcpip connection name> field of the Add or Modify TCPIP PCM command in the ClearPath MCP Software Custom Connect Facility Administration and Programming Guide for all possible station name values.*

When developing a station name, you need to consider uniqueness and determinability. For example, you might require that the station name be consistent each time a particular user connects, and will not change over time. You might also require that more than one connection be used from the same client or from any number of clients and each name used is unique.

You also need to consider any COMS security that is applied to station names and how these stations comply.

For the best means of ensuring a consistently unique name, use the <tcpip psnf> attributes $yourhost or $yourIPaddress within the stationname attribute value.

If a hostname is desired but an IP address is formed for the stationname instead, that is the letters **IP** are inserted in front of the address, it might be possible to use TCP/IP mapping to set the hostname. Refer to the *TCP/IP Implementation and Operations Guide* for more information on mapping IP addresses.

On some networks, such as Dynamic Host Configuration Protocol (DHCP), IP addresses are not consistent over time. In this situation there are two possible alternatives:

- Reserving a period of time where the IP address remains stable.
- Configuring a Domain Name Server (DNS) so TCP/IP can resolve an IP address to a known hostname.

  Refer to the *TCP/IP Distributed System Services (DSS) Operations Guide* for more information on configuring a DNS Resolver.

Overriding the Stationname by Client

When a station name is set by the client it overrides the configured setting defined for RATL connections above. Refer to the *Agile Business Suite Component Enabler User Guide* for more information on setting the station name by client. The station name supplied by the client might have a numerator applied to uniquely qualify the name, where multiple connections are desired from the same client. The numerator is represented by a string of one or more consecutive hash characters (#) appended to the station name which is converted to a unique ascending number. The number of consecutive hash characters indicates the minimum number of digits to be appended. For example, a supplied station name of user### results in names of the form: USER001, USER002, USER003 ... USER999, USER1000, USER1001 etc

The effect of StationName on station name (Glb.Stn)

The setting of the internal station name, or attribute Glb.Stn, is affected by the external (COMS) station name.

For Component Enabler (or NOF) based connections the value of Glb.Stn is based on the COMS station name value and the Remote Access service attribute StationNamePrefix value. If the StationNamePrefix is not defined then Glb.Stn is prefixed by the letters **RAT**, as shown in the first example below. If the derived station name is longer than the limit of 17 characters, the connection attributes for **yourhost** is used, as shown in the second example below. If the value for yourhost is not known or it is longer than the 17 character limit, the value for **youripaddress** is used. If this value is also too long the IP address is converted to its integer equivalent, as shown in the third example below.

The following example shows the resulting COMS and station names for a client with the specified Port Stationname format, a station name prefix set or not set to **SNP**, a hostname of Timbertown, and an IP address of 123.132.213.231:

TCPIP Port StationName	RATL Service StationName Prefix	COMS Station Name	Glb.Stn
ACTLINC/#	<null>	ACTLINC/1	RATACTLINC/1
	SNP	SNPACTLINC/1	ACTLINC/1
$yourhost/ $youraddress	<null>	TIMBERTOWN/1234	RATTIMBERTOWN/1
	SNP	SNPTIMBERTOWN/1234	TIMBERTOWN/1
$youripaddress/#	<null>	123_132_213_231/1	RAT2072303079/1
	SNP	SNP123_132_213_231/1	123_132_213_231/1

RATL Configuration

Configure the following entities:

- Service
- View
- Language

RATL Configuration Syntax

You can use the following verbs in CCF to configure the server for Component Enabler, or Web Enabler:

Verb	How it is Used
Add	To define attributes for Views, Languages, Services, MQservers, MQclients, and MQrequests.
Delete	To change existing Views, Languages, Services, MQservers, MQclients, and MQrequests. The View, Language, Service, MQserver, MQclient, or MQrequest must be disabled before it can be deleted or modified.
Disable	To change existing Views, Services, and MQrequests. The View, Service, or MQrequest must be disabled before it can be deleted or modified.
Enable	To enable existing Views, Services, and MQrequests.
List	To list Dialogs, Services, Languages, Views, MQservers, MQclients, and MQrequests.
Modify	To define attributes for Views, Languages, Services, MQservers, MQclients, and MQrequests. The View, Language, Service, MQserver, MQclient, and MQrequest must be disabled before it can be deleted or modified.
Option	To change server program runtime options.
Show	To show existing Views, Services, Languages, connected Dialogs, MQservers, MQclients, and MQrequests.
Status	To show the status of the PCM, such as compile time, code version, and title.
Trace	To alter or show the trace options.

Service

Identify a service to the PCM to associate the connection path for dialogs. Attributes are assigned using the following syntax:

```
Add Service <service name>
 service = <name>,
 NOFidentity = <name>,
 SwitchToFireUp = <boolean>,
 StationNamePrefix = <name>
Enable Service <service name>
```

Attribute	Description
<service name>	Defines a unique service name.

Attribute	Description
service	Specifies the name of a service to which inbound stations should be connected. This is the next service in the connection path. <name> must be a previously configured service.
NOFidentity	Identifies the connection types of the applications. <name> is a COMS Security Category List configuration entity that is defined in COMS. If the attribute is not configured in the service definition, it must be defined using the SecurityCatList attribute in the CUCI service definition before the server can handle the Component Enabler connections.
SwitchToFireUp	Specifies behavior when switching back to an application from which a switch previously occurred. This attribute is optional. If True, returns to the Fireup Ispec instead of the Ispec from which the original switch occurred. If False, returns to the Ispec from which the original switch occurred. If the client has not previously been displayed, the Fireup Ispec is retrieved. Any data contained in the SwitchTo command overrides the setting of this attribute.
StationNamePrefix	Prevents the RAT station name prefix appearing in Glb.Stn for Component Enabler connections. <name> prefixes the COMS Station Name. Refer to Using StationName. This attribute is optional.
MARCOpenText	Allows input to be passed to the MARC dialog when a new COMS connection is established from the server to a desired application. The value must be enclosed in double quotation marks. When this attribute is present the text is sent instead of the server passing a hard coded message to the MDPLAUNCH window. ***Note:*** *In order for the command to be carried out successfully by MARC, the CUCI Device attribute* ***marccapble*** *must be set to true.*

Example

```
Add Service RATL
 service = LINC,
 NOFidentity = SCL_NOF,
 SwitchToFireUp = False,
 StationNamePrefix = AL/
Enable Service RATL
```

Configuring Remote Access Server Entities

The Remote Access configuration entities for the COMS Security Category List names must be configured in at least one of the following attributes of the CCF configuration:

- SecurityCatList in the CUCI service definition
- NOFidentity in the service definition

Refer to RATL Configuration Syntax for more information about the syntax used to configure the server in an MCP environment.

When configuring entities you can change their names, but the names must remain unique. You can define additional Port and Service entities ensuring that a connection path can be resolved through CCF, encompassing the PCMs from TCIP using the Remote Access server to CUCI. Refer to the *ClearPath HMP NX/Services Administration Guide* or *ClearPath HMP Series CCF Administration Guide* for more information on using CCF.

View

You can identify Views to the PCM to associate connection criteria for Component Enabler users to access applications. A View can refer to one or more applications, or different Views might apply to the same application.

To identify at least one application, you can assign attributes using the following syntax:

```
Add View <view name>
 application = <system>,
 level = <number>,
 window = <name>,
 usercode = <usercode>,
 language = <language>
  comsstatuscheck = <boolean>
Enable View <view name>
```

Attribute	Description
<view name>	Specifies a unique view name.
application	Indicates the name of the initial application to be accessed through this View. This attribute is optional. <system> might contain the usercode, the application name and the Dictionary name of the built application. The Dictionary contains the LINCGLI, LINCFORM, and LINCCNTL files for the built application.
ComsStatusCheck	Specifies behavior when the transaction encounters a COMS Disabled Database on the MCP server. If True, an error 202 is returned to the client immediately. If False, the transaction will timeout.

Attribute	Description
level	Indicates the command level for dialogs using this View. This attribute is optional and only applies to NOF based connections.
window	Specifies the COMS window to be used by this View. This attribute is optional, but is required when the application to which you might need to switch is not already in use.
usercode	Indicates the usercode for every dialog that is established for this View. If it is not present, the client is asked for a usercode. This attribute is optional. <usercode> must be valid for the purposes of workstations connected to Runtime through COMS.
language	Indicates the preferred language to be used for this View. This attribute is optional. <language> must be a previously identified language.

Example

```
Add View sample_auto
 application = (USER1)SAMPSYS on DICTPACK,
 level = 0,
 window = SAMPLE
 usercode = anonymous,
 language = english
Enable View sample_auto
```

Language

Identify a language to associate the ISO Country code and an ISO Language code with a language name. The ISO Language code is defined in ISO 639 while the ISO Country code is defined in ISO 3166. These standards are available in the official ISO website, http://www.iso.ch/.

Language names are configured in the application. Attributes can be assigned and enabled using the following syntax:

```
Add Language <language>
 ISOC = <country code>,
 ISOL = <language cod
```

Attribute	Description
ISOC	Specifies the ISO Country code to be associated with the language name.
ISOL	Specifies the ISO Language code to be associated with the language name.

Example

```
Add Language english
 ISOC = EN,
 ISOL = EN
```

Message Queuing

Message Queuing allows multiple concurrent users of Component Enabler to access an Agile Business application, by making more efficient use of system resources, and reducing the overheads associated with establishing and maintaining individual connections for each user session. This is an alternative to the existing method of connecting to the Runtime application using individual TCP/IP connections.

Refer to the *Agile Business Suite Component Enabler User Guide* for more information on how to use message queuing for Component Enabler Scalability.

The following entities are added to the PCM section of the CCF params file to configure the request queues and connection details of the FalconMQ Server and FalconMQ Client library:

- MQServer
- MQclient
- MQrequest

MQServer

```
Add MQServer <name>
 Servername = <name>,
 IPaddress = <ipaddress>,
 Port = <number>,
 Domain = <name>,
 UserName = <name>,
 Password = <name>,
```

Set attributes associated with the FalconMQ server using the following syntax:

Attribute	Description
Servername	The name of the FalconMQ server. Default: <MQserver name>
IPaddress	The IPaddress of the FalconMQ server. An assigned IPaddress overrides any specified Servername.
Port	The required port number. Default: 0
Domain	The Windows security domain. Default: nulls

Attribute	Description
UserName	The Windows user name. Default: nulls
Password	The password associated with the Windows user name. Default: nulls

Note: *Case sensitive names that refer to a Windows entity can be enclosed by single quotes to prevent uppercasing.*

You can also use the following commands:

- Modify attributes of existing server entities

  ```
  modify MQServer <name>
     <attribute> = <value>,
  ```

- Itemize all declared MQServers

  ```
  list MQServers
  ```

- Display the attributes for the selected server

  ```
  show MQServer <name>
  ```

- Remove the selected server entity

  ```
  delete MQServer <name or list>
  ```

Example (*italics* denote responses):

```
   Add MQserver FMQS
    IPaddress = 123.1.2.3,
    Port = 1100,
    Domain = realm,
    UserName = dnote,
    Password = test,
  MQserver FMQS added
  Show MQserver FMQS
  1 FMQS
    IPaddress = 123.1.2.3
    Port = 1100
    Domain = realm
    UserName = dnote
    Password = test
```

MQClient

Set attributes associated with the FalconMQ client using the following syntax:

```
   Add MQclient <name>
    Functionname = <name>
```

Attribute	Description
Functionname	The System Library function name. Default: <MQclient name>

You can also use the following commands:

- Modify attributes of existing client entities.

```
modify MQclient <name>
  <attribute> = <value>,
```

- Itemize all declared MQclients.

```
list MQclient
```

- Display the attributes for the selected client.

```
show MQclient <name>
```

- Remove the selected client entity.

```
delete MQclient <name or list>
```

Example (*italics* denote responses):

```
Add MQclient FalconMQSupport
MQclient FALCONMQSUPPORT added
Enable MQclient FalconMQSupport
MQclient FALCONMQSUPPORT enabled
```

MQrequest

Set attributes associated with the request queue using the following syntax:

```
Add MQrequest <name>
 MQclient = <name>,
 MQserver = <name>,
 Pathname = <name>,
 Processes = <number>,
 Station Name = <SNformat>,
 Usercode = <identifier>,
 View = <name>,
 Service = <name>
```

Attribute	Description
MQclient	The name of the FalconMQclient.
MQserver	The name of the FalconMQ server.
Pathname	The request queue path name. Default: .\PRIVATE$\<MQrequestname>

Attribute	Description
Processes	The number of queue reader processes. Default: 1
Stationname	The pooling station name format. The possible Snformats are as follows: • <literal> • / • # • $ – – MQclient – – MQrequest – – MQserver – – ServerName – – IPaddress – – Domain – – Username Default: $MQrequest/#
Usercode	The pooling user code.
View	The name of the view. Default: <MQrequestname>
MQrequestname>	The service name. Default: <first service name defined (in Remote Access Server)>

You can also use the following commands:

- Modify attributes of existing MQrequest entities.

```
 modify MQrequest <name>
  <attribute> = <value>,
```

- Terminate the selected MQrequest reader process.

```
disable MQclient <name>
```

- Execute the selected MQrequest reader process.

```
enable MQrequest <name>
```

- Itemize all declared MSQclients.

```
list MQrequest
```

- Display the attributes for the selected client.

```
show MQclient <name>
```

- Remove the selected MQrequest entity.

```
delete MQrequest <name or list>
```

Example (*italics* denote responses):

```
Add MQrequest sampleQ
   MQclient = FalconMQSupport,
   MQserver = FMQS,
   Usercode = legion,
   View = samplesystem,
   Service = ratl
MQrepuest sampleQ added
List MQrequests
MQrequests:
1 sampleQ
```

COMS Configuration

To define connection types to applications, you need to define two COMS configuration entities. These are Security Category List and Installation Data entities. The names used in the CCF configuration for SecurityCatList (CUCI device attribute), and NOFidentity, should correspond to the names of Security Category List entities in the COMS configuration. Each Security Category List entity needs a corresponding Installation Data entity. The value assigned to the INTEGER1 attribute determines the type of connection for that entity. Currently, the only allowable value for INTEGER1 is 9.

You can define Component Enabler (NOF) based connection types for applications using the following COMS configuration entries:

```
CREATE INSTALLATION_DATA RATL_NOF
 INTEGER1 = 9
CREATE SECURITY_CATEGORY_LIST RATL_NOF
 ID = RATL_NOF
```

Remote Access Server Commands

Clear Command

This command is used to clear connections from the PCM.

Syntax:

```
Clear Dialog<#,name, or list>
```

Example:

```
Clear Dialogs 1,4-7,9
```

Option Command

The following list outlines the options users can set:

- AllAttributes
- ShowAsserts
- AssertDump
- CompactTables
- LogicError1
- LogicError2
- ForwardSyncMessages

  When set any received CCF Sync protocol messages are sent onwards, otherwise they are ignored.

  Syntax:

  ```
  Option [+/-] <option list>
  ```

  Example:

  ```
  Option +ForwardSyncMessages
  ```

- NoStationNameOverride

  When set prevents clients from overriding the station name configured for RATL connections. It can only be set in the CCF configuration file and its default value is off.

Administering the Remote Access Server

Administering the Remote Access Server involves the following tasks

- Starting and stopping
- Monitoring
- Security
- Tracing

Starting and Stopping

Use the CCF commands to start and stop the server and to monitor or trace server activities.

Note: *Any connections to COMS or a COMS application via NX Services (for example, NX view) are terminated.*

Because the server is configured as part of CCF, starting and stopping CCF starts and stops the server:

- To start Remote Access Server along with CCF, use:

  ```
  NA CCF+
  ```

- To stop Remote Access Server along with CCF, use:

  ```
  NA CCF-
  ```

Alternatively, the server can be started and stopped without disrupting CCF:

- To start Remote Access Server without affecting CCF, use:

  ```
  NA CCF enable pcm ratlpcm
  ```

- To stop Remote Access Server without affecting CCF, use:

  ```
  NA CCF disable pcm ratlpcm
  ```

Monitoring

You can monitor the status of any Remote Access server component configured in CCF, such as Languages, Views, and Dialogs. You can use the CCF **STATUS** or **SHOW** commands to display the status of the selected component.

The following example uses the **STATUS** command to display the status of the PCM. It displays the version, timestamp, internal program options and default language.

```
NA CCF RATLPCM STATUS
```

This command returns the following data:

```
Unisys Corporation COMSock
RATLPCM 44.201.1 -09/20/98 - 10:29:31
Compile Options:Trace, Assert
Language = ENGLISH
```

The following example uses the **SHOW** command to display the status of the connected dialog.

```
NA CCF RATLPCM SHOW DIALOG 1
```

This command returns the following data:

```
Sunday 09/20/98 10:29:31
1 RATL/UNO
Client = Open
Transport = Open
Service = Open
Input Seq Num = 8
Output Seq Num = 6
NOF = True
GUI = False
View = UNO
Language = SPANISH
Device = RATLWEB
Maxoutput = 6000
HostName = ACUSAHA
ACVT = Default
```

Security

If a host application supports password aging and the Remote Access server is compliant with the application then user passwords can be changed when using the Remote Access server.

Refer to the *MCP/AS Security Administration Guide* for more information on setting password aging on an A Series host.

Tracing

Use CCF commands to start and stop tracing and to set the tracing attributes. Tracing can be initiated either by the operator, or by the client as part of the connection request. Tracing is normally used only for problem resolution, as it might impact the performance of the server.

The options for the CCF TRACE command are:

ON or RESUME	Turns tracing on.
OFF or SUSPEND	Turns tracing off.
CLOSE	Closes the current trace file.

You can set trace attributes to specify which activity is traced. The trace attributes are listed in the following table:

Attribute	Components Traced
RATL	RATL protocol
ALLDLGS	All dialogs
Attach	Session establishment and termination
Blocked	Suspended and resumed output
CMDINFO	CCF command data buffer
CREDITS	Bytes available for transmission
DATAINFO	CCF associated data buffer
DATAPATH	Procedural flow of message buffering
FULL	Shows full size of data buffers
LISTBUFS	Internal data space processing
LOCKS	Contention
MISC	Miscellaneous
MISCPROCS	Miscellaneous processing
MQ	Message Queue interface
MSG	Message displays
OPERINP	Operational interface
PFD	Configuration file parameters
SCANNER	Parsing

Attribute	Components Traced
TBL	Tables

An example of the CCF command to start tracing all dialogs for the Remote Access server is as follows:

```
NA CCF RATLPCM TRACE ON +ALLDLGS
```

Remote Access Server Protocol Response Messages

In particular situations the server sends protocol messages, with a number of possible response codes, to the client.

The following table outlines some of the more common codes and possible causes, to assist in determining the cause of the message:

Response Code	Meaning	Possible Causes
100	Successful operation	Session was successfully established.
101	Login is required	The View does not contain a usercode attribute setting.
103	Additional login	The userdata file indicates that other required user related attributes are needed.
201	Application does not exist	Either the View is not known to the server or the application referred to in the View does not exist.
203	Application cannot be contacted	Unable to read or obtain the desired information from the control file.
204	Access denied	• Application is not EAE 3.3 or later release. • Userdata validation error (invalid usercode/password). • Duplicate connection name. • Usercode specified on View does not exist or is not valid. • COMS Window for the Application does not exist or is not valid (window list). • Security Category List used by connection does not exist in COMS. • Failed COMS Usercode/Station name security checking.

Localization of Messages

Remote Access Server messages can be translated using the MCP-based Multilingual System (MLS). The user messages are stored in the program SYSTEM/LINC/PCM/RATL in the following arrays:

- pcm_msgs
- login_prompts
- login_labels

Configuring TLS 1.2 Remote Access Server

A TLS certificate must be installed on the server to ensure a secure connection and protect all important information. You must first create a TLS 1.2 certificate on the MCP host machine before importing the security certificate using Security Center.

Notes:

- *Earlier TLS and SSL levels are not supported due to known vulnerabilities. Only TLS 1.2 level is supported.*
- *In the following procedure, the use of the terminology **SSL** for service and parameter names is due to the use of pre-existing frameworks and must not be read as SSL support.*

To configure the TLS Remote Access Server, perform the following:

1. Create the TLS certificate request on the MCP host machine:

   a. Ensure that the Security Center must be installed on the host and a PC environment.

      Refer to the *MCP Security Overview and Implementation Guide* for more information.

   b. To open the Security Center, select **All Programs** > **Unisys MCP** > **Security Center**.

   c. Select **MCP Cryptographic Services Manager** > **Trusted Keys**.

   d. Right-click on **Other Keys**, and then select **Create Key**.

   e. Set the Application to **CCF** and the Service name to **RATLKEY**.

   f. Set the Usercode to ***NULL** and key strength to at least 2048.

   g. Select the **Create Certificate Request** check box, and then fill in the remaining fields with the appropriate details (for example, Signature Algorithm is SHA256_RSA).

      Refer to the *Online Help* for more information.

   h. Click **OK**.

      The **Save** dialog box is displayed.

   i. Enter the file name, and then click **Save**.

This creates a certificate request file (.req).

Note: *It is recommended that this certificate request file must be processed by a trusted third-party Certificate Authority (CA).*

2. Import the security certificate:

   a. Open the **Security Center**.

   b. Select **MCP Cryptographic Services Manager** > **Trusted Keys**.

   c. Expand the key store where the key was created.

   d. Right-click the key, and then select **Options** > **Install Certificate Into Set**.

   e. In the File Browser, select the **.P7B** or **.P7C** file.

      When the certificate is successfully installed a green check mark appears next to the name of the certificate.

      Note: *If you are using a non-trusted CA, the created .P7B or .P7C file will be ready for installing or importing on the client. This same process must be followed if you are using a self-signed certificate.*

3. Configure the RATL TLS port:

   The supplied file NGEN28/SAMPLE/CCF/PARAMS/RATL contains the necessary configurations for RATL TLS. These must be customized to suit your environment.

   The added configurations are

   a. PORT RATLSSL

      As per PORT RATL with the additions/change of:

      SOCKET = 2018, % choose the socket number

      SSLSECUREMODE = TRUE, % always

      SSLKEYCONTAINER = CCF_RATLKEY; % the key name, this must be the concatenation of the two names used in 1 (e) above using a '_'.

   b. SERVICE RATLSSL

      As per SERVICE RATL

      Additionally, TLS must be enabled on TCPIP.

      From MARC: NW TCPIP OPT +SSL

Refer to the *MCP Security Overview and Implementation Guide* and *TCP/IP Distributed Systems Services Operations Guide* for more information on MCP security.

Installing and Configuring Remote Subroutine Server

The Remote Subroutine Server (also known as LRSS) enables Debugger to call subroutines from host Runtime platforms.

There are two methods of installing Remote Subroutine Server:

- You can install it as part of the standard installation of Runtime software (refer to Installing the MCP Runtime Software).

- You can install it independently using the LRSS install WFL.

Independent Installation

To install the Remote Subroutine Server, enter the following command:

```
START NGEN28/SAMPLE/LRSS/INSTALL ("usercode","packname")
```

The location of the files is based on the current directory. A Usercode and Pack name might be provided as optional parameters to the install job.

The install job performs the following:

- Registers the Remote Subroutine Server as a Distributed System Services (DSS) provider
- Maps the Support Library (SL) function names for Remote Subroutine Server

Alternatively, the installation can be performed manually. Use the following commands from the system console or a suitably privileged station:

1. To register Remote Subroutine Server as a DSS provider enter the following command:

   ```
   NA LOAD COMMANDS LRSS/DSS/REGISTER
   ```

2. To map Support Library (SL) function names for Remote Subroutine Server enter the following command:

   ```
   SL LRSSSUPPORT= SYSTEM/LRSS/SUPPORT: TRUSTED, LINKCLASS= 1
   SL LRSSPDUSUPPORT= SYSTEM/LRSS/PDUSUPPORT: TRUSTED, LINKCLASS= 3
   ```

Note: *Usercode and Pack names might need to be inserted into the above commands as applicable.*

Configuration

To configure Remote Subroutine Server you need to set the options in the configuration file that is read at startup. The file is at LRSS/CONFIG and all options have default settings, so users only need to change them if the need arises.

The options are:

```
PORT =                    <Integer, 0 to 65535, default 6004>

CONNECTIONS =             <Integer, 1 to 4000, default 12>

MAXOFFER =                <Integer, 1 to 99, default 1>

INACTIVITY =              <Integer, 1 to 1440, default 10 minutes>

TIMEOUT =                 <Integer, 1 to 1440, default 60 minutes>

ERRORS =                  <File name, default LRSS/ERRORS>

TRACE =                   {ON | OFF (default) [[TO] <File name, default LRSS/
                          TRACE/#>]}
```

These options are:

- **PORT**

  The Port is the TCP/IP communications service number used to establish incoming connections from prospective clients.

- **CONNECTIONS**

  Connections is used to limit the total number of concurrent sessions available.

- **MAXOFFER**

  MaxOffer controls the number of listening port subfiles that are available. The range is either 1 through 99, or 1 through the number of connections allowed (if less than 99).

- **INACTIVITY**

  Inactivity is the interval of time between when TCP/IP keep alive packets are exchanged with the client. The inactivity value is mapped to the port file attribute DialogCheckInterval.

- **TIMEOUT**

  Timeout is the duration for which TCP/IP keep alive packets can continue to be sent before a connection is closed. The range is as applicable for the port file attribute BlockedTimeout.

- **ERRORS**

  The Errors option locates the filename for any configuration problems found. Messages are logged to the error file with a reference to the problem line in the configuration file.

- **TRACE**

  Trace is available for observing Remote Subroutine Server behavior or diagnosing problems. Tracing can be turned on or off, and the title of the trace file can also be set. The default value is off and the default title is LRSS/TRACE/#, where # is a numerator starting at zero. Each time the server starts, the trace file name’s numerator restarts at zero.

- **Comments**

  Comments can be placed anywhere in the text stream and are terminated by the end of each line. A comment is denoted by the presence of either a percent or an asterisk character in the text stream except when enclosed by quotation marks.

  The syntax is as follows:

  ```
  % this is a comment* and so is this
  ```

Operations

Remote Subroutine Server can be controlled through the Network Application (NA) interface. You can start, stop, show status or change trace options. These commands are:

Action	Command
Start	NA LRSS +
Stop	NA LRSS -
Show Status	NA LRSS STATUS
Trace	NA LRSS TRACE [ON I OFF I Release]

When the Release option is used on the trace command, the existing trace file is closed and a new trace file is opened with an increment to the numerator portion of the trace file title.

If Remote Subroutine Server is not running, it starts automatically when an incoming connection is attempted on the port service number registered through DSS for Remote Subroutine Server.

Monitoring

A facility exists in Remote Subroutine Server to monitor remote method calls made from its clients. The monitor facility is programmatically interfaced and provision is given to veto any remote procedure calls at hand.

Monitoring depends on the entry point within a user written application. For the monitor to work a Support Library (SL) named LRSSMONITOR must exist. This SL is checked for at startup.

The entry point is described, and an example given, in the sample source file **LRSS/MONITOR**.

Setting up FTP

Set up FTP to allow access to the usercode from Builder. Use the following SYSTEM/ MAKEUSER +RU commands:

```
+RU *ANYUSER OF *IPADDRESS nnn[.nnn[.nnn[.nnn]]]
+RU usercode OF *IPADDRESS nnn[.nnn[.nnn[.nnn]]]
```

Where nnn[.nnn[.nnn[.nnn]]] contains the required IP address nodes.

Perform the following to use Secure FTP (TLS 1.2) for the file transfer from the PC to the MCP host:

1. Create the TLS certificate request on the MCP host machine:
    a. Ensure that the Security Center is installed on the host and in a PC environment.

       Refer to the *MCP Security Overview and Implementation Guide* for more information.

    b. To open the Security Center, select **All Programs** > **Unisys MCP** > **Security Center**.

   c. Select **MCP Cryptographic Services Manager** > **Trusted Keys**.

   d. Right-click on **WebTS Keys** and then select **Create Key**.

   e. Set the Service name to **FTPTLS**.

   f. Set the Usercode to *NULL and key strength to at least 2048.

   g. Select the **Create Certificate Request** check box, and then fill in the remaining fields with the appropriate details (for example, Signature Algorithm is SHA256_RSA). Refer to the *Developer Online Help* for more information.

   h. Click **OK**.

      The Save dialog box is displayed.

   i. Enter the file name and then click **Save**.

      This creates a certificate request file (.req).

      Note: *It is recommended that this certificate request file be processed by a trusted third-party Certificate Authority (CA).*

2. After the .certificate request (.req) has been processed by the CA, import the resulting security certificate

   a. Open the **Security Center**.

   b. Select **MCP Cryptographic Services Manager** > **Trusted Keys**.

      Expand the key store to where your key was created (WebTS Keys).

   c. Right-click on your key, and then select **Options** > **Install Certificate Into Set**.

   d. In the File Browser, select the appropriate .P7B or .P7C file.

      When the certificate has been successfully, a green check mark appears next to the name of the certificate.

      Note: *If you are using a non-trusted CA, the newly created .P7B or .P7C file is now ready for installing or importing on the client. The same process must be followed if you are using a self-signed certificate.*

3. From MARC, enable SSL on TCPIP: NW TCPIP OPT + SSL % to ensure SSL lib is active.

4. Configure the FTP properties in the FTP configuration file —

```
*SYSTEM/FTP/SUPPORT/CONFIGURATION
```

   a. Apply these changes to the FTP configuration file:

```
    (1) AUTHMODE = SSL
    (2) SSLMODE = IMPLICIT
(3) SSL_SERVICENAME = “FTPTLS”  %your WebTS Key name from above
    (4) INITIATE_SSL_SERVER = 1
    (5) CLIENT_CERTIFICATES = NONE
```

   b. Save the updated FTP configuration file.

   c. Restart FTP

From MARC,

`NA FTP` – followed by

`NA FTP +`

Refer to the *MCP Security Overview and Implementation Guide* and *TCP/IP Distributed Systems Services Operations Guide* for more information on MCP security.

Refer to Installing Windows TLS Certificate for instructions on importing the FTP certificate into the Windows Trusted store.

Installing the MCP Runtime IC to a new environment

Notes:

- *If you are installing to environments used in Runtime Transfers, you must install the release from the same installation package in both the source and target runtime environments.*
- *Where you see <IC number> in the instructions below, use the IC number from the container file, which has the format nnnn-nn.*

If this is the first time that the runtime is being installed in the designated runtime usercode and you have not installed the GCA release already, follow these steps

1. Logon to your privileged usercode

   ```
   START NGEN28/WFL/RUNTIME
   ```

   (”*usercode*”,”*pack*”,”*alias pack*”,FALSE,

   ”*GCA media parameter*”

   ”*IC media parameter*”)

   The *usercode* value is the usercode to which the Runtime is installed, which might be an asterisk (*).

   The *pack* value is the family name of the pack to which the Runtime is installed, which might be DISK or altpack.

   The *aliaspack* value is the pack for your station alias file. Refer to the *Agile Business Suite Runtime for ClearPath MCP Administration Guide* for more information on station aliases.

   GCA media parameter = “MD=*MediaDirectory* MN=*MediaName* N=*1000-02*"

   MediaDirectory is the directory containing the installation files:

   EPSILON

   ```
   (TRANSFER)GCA
   ```

   ETA

   ```
   (TRANSFER)ETA/GCA
   ```

MediaName is the name of the pack on which the installation files are located.

<Transfer pack>

For example:

"MD=(TRANSFER)ETA/GCA MN=TFRPACK N=1000-02"

IC media parameter = "MD=*MediaDirectory* MN=*MediaName* N=*Cut#*"

MediaDirectory is the directory containing the installation files:

EPSILON

```
(TRANSFER)IC
```

ETA

```
(TRANSFER)ETA/IC
```

MediaName is the name of the pack on which the installation files are located.

<Transfer pack>

Cut# is the IC number.

<IC number>

For example:

"MD=(TRANSFER)ETA/IC MN=TFRPACK N=1001-01"

Notes:

- *The usercode from which the RUNTIME job is started must be privileged.*

  If the RUNTIME job is started from a non-privileged usercode, any SLs for libraries released with this cut must be done manually from MARC under a privileged usercode.

- *If your machine has Security Administrator status enforced (by enabling the SECADMIN option), the usercode from which the RUNTIME job is started must have SECADMIN privileges.*

  If the usercode does not have SECADMIN privileges, any SLs for libraries released with this cut must be done manually.

2. Start the Runtime WFL, by entering:

3. License Agreement – Before the installation begins, you will be asked to accept the license agreement. The installation job is suspended twice to allow you to read the license information. The terms of the license agreement might be found in the instruction blocks. Enter ?IB nn from MARC to view each instruction block. Enter ?OK to accept the license agreement and install Agile Business Suite 7.0 for the MCP Operating System.

4. During the installation, you will be asked

   ** DO YOU WISH TO OVERWRITE EXISTING LIBRARIES (HUBROUTER, RATL, ETC.) WITH THE LIBRARIES IN THIS RELEASE? AX YES TO OVERWRITE OR AX NO TO INSTALL/RETAIN LATEST VERSION **

   This allows you to overwrite existing libraries, even if their release level is higher than the GCA release. Respond with AX YES to overwrite existing libraries.

Respond with AX NO to allow the installation job to use release checking and only install the new libraries if they have a higher release level than the existing libraries.

5. During the installation, you will be asked to confirm the version of AB Suite 7.0 MCP Runtime that is being installed.

   Respond with OK to confirm.

   DS the job to terminate the installation.

6. Go to Responding to Prompts during the Installation

Deploying the First Application After Installing Runtime

The instructions in this topic are applicable to the first deployment of your application after installing the Runtime for the first time.

> **Caution**
>
> After installing the Runtime, disable your application system for the duration of the deployment phase of the build to avoid duplicate LINCSUPPORT libraries from appearing during the hotswap phase of the system deployment and to activate new code files.

The below instructions describe the process of disabling the system during deployment with minimum downtime. It is important for you to read the instructions carefully.

The Delay Compile and Deploy option on the Host Login dialog box is used in conjunction with a system built with the Rebuild option to minimize the system downtime. For those who do not want to use the Delay Compile and Deploy option, refer to Deploying the System without Delaying the Deployment.

It is essential that each step be performed to avoid problems during this deployment or problems in the system after the deployment.

Deploying the System with Minimal Downtime

This method of deployment results in the system being down for a minimal time. The Delay Compile and Deploy option is used to suspend the deployment, after the generate phase is complete, to provide an opportunity to disable the system. The deployment is suspended at the point of deployment or at the point of installation.

To deploy your system with a delayed deployment, perform the following:

1. As part of pre-build preparation, remove your BuilderCache and BuilderOutput directories.

2. (Optional) Add your system and critical reports to the APPL_BLD server. Use the DELAYINSTALL APPL_BLD command to cause the deployment to wait at the point where the installation (Generate WFL) starts if the Delay Compile and Deploy option is used. Skip this step if you prefer the deployment to be suspended at the point of initiating the Compile phase.

   a. Add System to APPL_BLD Server. Enter this command from the MARC Action field.

      ```
      NA APPL_BLD_<ident> ADDSYS  NAME=<system name>
      USER=<usercode> PACK=<pack>
      ```

      Where <ident> is the identity of APPL_BLD.

      Refer to the ADDSYS command in the *Agile Business Suite Runtime for ClearPath MCP Administration Guide*.

   b. Get the index number for the system. Enter this command from the MARC Action field.

      ```
      NA APPL_BLD_90 INDEX
      ```

   c. Note the index number for the system from the results of the inquiry in Step b.

   d. Add Critical reports to the APPL_BLD Server. Enter one of the following commands from the MARC Action field.

      ```
      NA APPL_BLD_<ident> ADDREP  <nn> =
      <report name>[, <report name2>. .]
      NA APPL_BLD_<ident> ADDREP  <nn> #<file title>
      ```

      Where:

      <ident> is the identity of APPL_BLD.

      <nn> is the system index noted in Step b.

      <report name> and <report name2> are the names of reports.

      <file title> is the name of a file that contains a list of reports.

      Refer to the ADDREP command in the *Agile Business Suite Runtime for ClearPath MCP Administration Guide*.

   e. Set DELAYINSTALL option for the system in the APPL_BLD Server. Enter this command from the MARC Action field.

      ```
      NA APPL_BLD_<ident> DELAYINSTALL  <nn>
      ```

      Where <ident> is the identity of APPL_BLD, and <nn> is the system index that you noted in Step b.

      Refer to the DELAYINSTALL command in the *Agile Business Suite Runtime for ClearPath MCP Administration Guide*.

3. Start the deployment.

   a. Right-click the deployment folder and select **Rebuild** or **Folder Only Rebuild**.

   b. On the **Host Login** dialog box, enter the login details.

c. Select the **Delay Compile and Deploy** option.

d. Change the Deploy Date and the Deploy Time to a suitable date and time in the future.

Allow sufficient time for the Build phase to complete and for you to disable the system. Include additional time if you perform Step 2. It is recommended to change the Deploy Date and Deploy Time to a day after the expected completion of the Generate phase.

e. Click **OK**.

4. Verify that the generate phase on the client is complete and the deployment of the system is queued on the MCP server.

   The Generate phase on the client is finished when the following message appears in the log.

   ```
   The System Generate has been delayed until a later time
   ```

   Systems queued for deployment can be viewed from the APPL_BLD server using the following command.

   ```
   NA APPL_BLD_<ident> QUEUE
   ```

   Where <ident> is the identity of APPL_BLD.

   For default installations of APPL_BLD, <ident> is 90. For example, APPL_BLD_90.

   The message returned by the QUEUE command is a list of queued systems.

   ```
   1.  17:30:00 on 17/02/2023,Scheduled,
   System MYUSER,MYSAMPLE,MYPACK
   ```

   Take note of the queue number for the system. It will be used in Step 6 to resume the deployment. The queue number for the example system above is 1.

   Note: *If you do not see the queue number and you performed Step 2, there will be a waiting entry about the delayed installation and the installation will be in the job queue.*

5. Disable the system.

6. Resume the queued deployment.

   a. If you did not perform Step 2 and found a queued generate, then perform the following steps:

      From MARC, enter the command.

      ```
      NA  APPL_BLD_<ident>  FORCEQ  <n>
      ```

      Where <ident> is the identity of APPL_BLD.

      For the default installation of APPL_BLD, <ident> is 90. For example, APPL_BLD_90.

      <n> is the number assigned to the queued deployment.

      Use the number you obtained from Step 3.

      For example, from MARC enter:

      ```
      NA  APPL_BLD_90  FORCEQ  1
      ```

The message returned from this command is as shown below.

```
Queue entry #1 set to now
```

b. If you performed Step 2 and did not find a queued generate, perform the following:

   Use the information in the waiting entry to find the job for the installation (Generate WFL) in the queue and force the job from the queue.

```
<mix> FS
```

7. If you use non-default MAXWAIT values, reapply them after the system has been deployed.

   The default MAXWAIT settings are as follows.

```
COMS_LINC_TP          30 seconds
LSS                   10 seconds
```

8. Deploy system critical reports with the REBUILD option.
9. Enable the system.
10. Deploy remaining reports with the REBUILD option.

Deploying the System without Delaying the Deployment

If you do not want to use the Delay Compile and Deploy option to suspend the deployment, you can disable your system before starting the build. To build your system without delaying the deployment, perform the following steps:

1. As a pre-build preparation, remove your BuilderCache and BuilderOutput directories.
2. Disable the system.
3. Right-click the deployment folder and select **Rebuild** or **Folder Only Rebuild**.
4. On the **Host Login** dialog box, enter the login details.
5. Click **OK**.
6. On completion of the deployment, reapply MAXWAIT values.
7. Build system critical reports with the REBUILD option.
8. Enable the system.
9. Build remaining reports with the REBUILD option.

Updating the System with MCP Runtime Transfer

To update the system with MCP runtime transfer:

1. Build the source or base system using one of the sets of instructions described above. Refer to Deploying the System with Minimal Downtime or Deploying the System without Delaying the Deployment for more information.
2. Build the Runtime Transfer Utility (RTU) file with the **Rebuild** option.

Note: *You might want to perform this step as part of Step 1. Ensure that the Runtime Transfer properties are set up correctly before you Rebuild the Source System.*

3. Perform the following mandatory steps for transfers using Hands Free Configure or Compile Free Configure.

    - If you are using Hands Free Configure, the compile phase starts automatically. As such, it is necessary to disable the Target System.

    - If you are using Compile Free Configure, the system libraries are compiled during the transfer phase. As such, it is necessary to disable the system.

        a. Disable Target System. (For an RDB system, disable the Primary System.)

        b. For RDB Systems, check the status of the RDBSUPPORT library for the Primary System and secondary database. If it is not leaving the mix, check whether it is still linked to NGEN30/1/LIBRARY (function name NGEN30SERVICES). If it is still linked to RDBSUPPORT through NGEN30/1/LIBRARY, delink it by using the DELINK RDBSUPPORT command for NGEN30/1/LIBRARY (use the mix number for the control library).

    Note: *For the transfers that are not using Hands Free Configure or Compile Free Configure, the above steps are optional.*

4. Initiate RTU by entering the command:

    ```
    R $(<runtime usercode>)NGEN30/RTU ON <runtime pack>;
    ```

5. In the Transfer Startup screen, enter the <<segment>> class and configuration sets associated with the transfer.

6. In the Transfer Selection screen:

    a. Enter Y in the Tfr/Configure All Ispec Code field.

    b. In the Auto initiate configure program field:

    Enter N in the Auto initiate configure program field if the Target System is not disabled at this point. Do this regardless of whether you use BNA as the transfer medium or not. It is necessary to disable the target system before you deploy it. It will be easier to do this if the Configure phase is not started automatically.

    Enter Y in the Auto initiate configure program field if the Target System is disabled at this point. You will be using BNA as the transfer medium and use Hands Free Configure. If the Target System is still enabled but you want to use Hands Free Configure, perform the tasks in Step 3 to disable the Target System.

    c. Change the rest of the options on this screen as you would for a normal transfer at your site. The transfer should include the reports.

7. In the Transfer Creation screen:

    a. Enter Y in the Auto initiate of transfer job field. The transfer phase will be initiated by RTU.

    b. Change the other options on this screen as you would do for a normal transfer at your site.

8. If the Selected Transfer screen appears, set up the options so that both the system and reports are transferred.

9. Transmit the final screen in RTU. The Transfer phase starts after you transmit the final screen in RTU. Wait until this phase is complete and the transfer files have been transferred to the transfer medium.

10. For the transfers that do not use Hands Free Configure or Compile Free Configure, if the Target System (or Primary System) is not disabled already, it must be disabled now.

    a. Disable the Target System. (For an RDB system, disable the Primary System.)

    b. For RDB systems, check the status of the RDBSUPPORT library for the Primary System and secondary database. If it is not leaving the mix, check whether it is still linked to NGEN30/1/LIBRARY (function name NGEN30SERVICES). If it is still linked to DBSUPPORT through NGEN30/1/LIBRARY, delink it by using the DELINK RDBSUPPORT command for NGEN30/1/LIBRARY (use the mix number for the control library).

11. Run the Configure Utility for the transfers not using Hands Free Configure.

    ```
    RUN $RUNTIMETRANSFER/<source config>/
    <target config>/CONFIGURE
    ```

    (for an automated configure using a configure configuration set)

    OR

    ```
    RUN $RUNTIMETRANSFER/<source config>/CONFIGURE
    ```

    (for a manual configure using the Configure Utility screens)

    The Configure Utility will initiate the configure phase for transfers that do not use Hands Free Configure.

12. Wait for the configure phase to complete, and then enable the system.

13. For RDB systems, if there is a Standby System in the RDB system, transfer the Primary System to the Standby System.

```
If the RDB system does not have a Standby System, but reports are
run against the secondary database, transfer reports from the
Primary System to the secondary database.
```

Migrating to Release 7.0

Migration Procedure

Agile Business Suite Release 7.0 does not include Host Builder. If you are still using Host Builder in releases prior to 3.3, you must first migrate your application to Developer, following the instructions in the *EAE to Agile Business Suite Migration Guide*.

You must then migrate your application from 3.3 to Agile Business Suite 7.0 following the instructions in the *EAE 3.3 to Agile Business Suite Migration Guide*.

Notes:

- *Change in naming convention – In previous products, the naming convention for the first node in the directories for the runtime software has been LINCxx and LINCxxSYS. For example, LINC17/LSS, LINC17/1/LINCSUPPORT, LINC17/WFL/ GENERATE, LINC17SYS/BLD, etc. The naming convention for these directory nodes is now NGENxx and NGENxxSYS. For example, NGEN28/LSS, NGEN28/1/ LINCSUPPORT, NGEN28/WFL/GENERATE, NGEN28SYS/BLD, etc. If you have jobs or non-EAE applications that refer to any of these files, you must change the first directory node from LINC17[SYS] to NGEN28SYS].*

  The naming convention for two SLs has also changed. LINCxxSERVICES is now NGENxxSERVICES. For this release it is NGEN28SERVICES. LINCxxMLSSUPPORT is now NGENxxMLSSUPPORT. For this release it is NGEN28MLSSUPPORT.

- *User GLI programs – If your existing user GLI programs are sending data to ispecs that have the system MAINT field present (standard ispec or a memo ispec with an automaint profile) then you must change the field name MAINT to USERMAINT.*

- *For applications that use the Remote Access Server and are being migrated from EAE, it is necessary to disable and enable CCF after the application has been deployed from AB Suite. This ensures that the RATL view for the application reads the new LINCCNTL file.*

Using the USS5100 Unisys Remote Data Facility

The USS5100 Unisys Remote Data Facility (URDF) is a disk mirroring system that can be used to provide a remote copy of an application for disaster recovery backup purposes.

The following issues should be considered when using the URDF with systems:

- Capabilities within MCP based software in order to optimize data recovery
- Minimize system downtime in the event a switch to the remote system becomes necessary

Planned Recovery

Planned recovery indicates that the application has been successfully taken to EOJ the source host.

The following table shows the non DMSII files that require mirroring:

File	Family
Linccntl	Dictpack
Linclog	Logpack
Unique/Save	Dictpack
Extract files	Extractpack

File	Family
Roc Data Files	Rocpack

There are a number of files that must be synchronized between hosts, based on the assumption that the alternate family (DISK) or the backup family (PACK) is not mirrored across hosts.

These files and disk families are shown in the following table.

File	Family
*Coms/Cfile	Disk
*Coms/Cfile	Disk
*Linc/Stn/Alias	Disk

In addition, the development or runtime environments must also be present on both hosts. Having this software loaded ensures the system-wide runtime libraries are always available.

Online Application Takeover

Planned Takeover

In the case of a planned takeover, before you attempt to log into the application on the secondary host, perform the following:

1. Ensure that the latest *system*/COMS/CONFIG/FULL file details are contained in the *COMS/CFILE.

   If you are unsure, load this file (located on the dictionary pack) via the COMS batch load facility on the Utility window.

2. If the system has COMS Protected Output and Protected Input enabled, as a precaution, you can disable COMS recovery. To do this:

   - Go to the DRC window of the COMS Utility.
   - Set Create New file to *Y*.
   - Set RDS pointer to end to *Y*.

3. Log into the application. The normal application startup should proceed.

During the takeover, if you log back into the application with a different terminal id, then a new Glb-Dialoginfo record is created. If this occurs, you might want to maintain the same Installation Data across the Configuration files on both hosts. This ensures that when a user logs in to either host, the same privileges are granted by both hosts.

Unplanned Takeover

In the case of an unplanned takeover, before you attempt to log into to the application window on the secondary host, perform the following:

1. Ensure the latest *system*/COMS/CONFIG/FULL file details are contained in the *COMS/CFILE.

   If you are unsure, load this file (located on the dictionary pack) via the COMS batch load facility on the Utility window.

2. If the application has COMS Protected Output and Protected Input enabled, as a precaution, you can disable COMS recovery. To do this:

   - Go to the DRC window of the COMS Utility.
   - Set Create New file to *Y*.
   - Set RDS pointer to end to *Y*.

3. Log into the application. At this stage *SYSTEM/DMRECOVERY is started to recover the database. If there are any DMSII recovery issues, refer to your DMSII Utilities manual.

Notes:

- *Once DMRECOVERY is complete, LSS restarts any Reports that were running at the time of the takeover. Refer to Report Recovery During Unplanned Takeover for more information on this phase of recovery.*
- *The application attribute Glb.Unique value is increased by 2,500 from the value contained on the source host before the takeover.*
- *The LINCLOG will have lost a number of records, depending upon when the log buffer was last flushed. If the LINCLOG is critical to your application, it might be necessary to implement procedures where the LINCLOG is regularly released to minimize the impact of losing any records.*

During the takeover, if a user logs back in to the application with a different terminal id, a new Glb-Dialoginfo record is created. If this is the case, it would be good practice to ensure the same Installation Data is maintained across both hosts' Configuration files. This ensures that when the user logs on to either host, the same privileges are granted.

If the user logs back with a different terminal id, the last screen might not be able to be recalled, and the following error is displayed:

```
MESSAGE NOT AVAILABLE FOR RECALL; ERROR
```

This also indicates that the last instance of Glb.Work is no longer available.

Unplanned Takeover during Reorganization or Application Build

If an unplanned takeover occurs during a reorganization or an application build, it is necessary to:

- Reload the application from the latest backups.
- Start the reorganization or build from the beginning.

Report Recovery During Unplanned Takeover

Reports are restarted by LSS when the SYSTEM/DMRECOVERY completes on the secondary application.

In the following two cases, the Reports were all restarted with Critical Points. If any Reports that do not contain Critical Points are restarted, then those Reports are run from the beginning. Consequently, all Report output is started from the beginning.

Reports Creating Extract Files

The Report restarts from the last Critical Point, and if the Extract pack is mirrored, the Extract file continues writing records from the last record written at the Critical Point.

Reports Using ROC Flat Files

The Report restarts from the last Critical Point, and if the ROC data pack is mirrored, the Report continues writing records from the last record written at the Critical Point.

You should take care when the Report completes, or the Report is released for printing, because the ROC sleeping Report attempts to route the Report back to the source host for printing. At this stage, the source host might not be available.

It might be necessary to set ROC to 0, and when the Report completes, send it to a new destination using the ROC Inquiry screens. This only applies to restarted Reports.

Reports Writing Directly to a Printer Backup

The Report restarts from the last Critical Point. It is unlikely that the backup family is mirrored, in which case the Report output completed at the last Critical Point is on the backup family of the primary host, which might not now be available. All new output from this restarted Report is written to the backup family on the secondary host.

Appendix A
Installing Interim Corrections

An Agile Business Suite Interim Correction (IC) is a software package that is designed to distribute fixes and updates for the General Customer Availability (GCA) version of the Development Environment, Client Environment, and Runtime.

If the GCA version of the Development Environment and Runtime is not detected, Browse to GCA path dialog box appears. You can browse to the Development Environment subfolder (or the equivalent Windows Runtime subfolder for a Runtime installation) in the AB Suite installer and follow the wizard instructions. The IC can then be installed using the license provided in the GCA, without actually installing the GCA version. This allows clean installs of an IC without having to install old versions of the product first.

For the MCP Runtime, the following message appears, if you try to install the Runtime from an IC and the GCA release is not detected. For information on installing an IC for MCP Runtime, see Installing Interim Corrections for Runtime for ClearPath MCP.

```
>>> (<usercode>)NGEN30/AUTHENTICATE ON <pack> IS MISSING OR INVALID <<<
COPY VALID AUTHENTICATE FILE FROM THE GCA RELEASE: AX TO CONTINUE OR DS
```

Note: *You can directly install an IC release on a clean machine without the GCA version being installed. If there is no GCA version installed, the IC runs as a new base installation.*

Interim Corrections are distributed on the support web site for the product at:

https://www.support.unisys.com/common/ShowWebPage.aspx?id=1046&pla=ABS&nav=ABS

They are available as zip files for download. Once you have downloaded and saved the appropriate Interim Correction file, to a temporary location, to update your installed application, perform the following:

1. Extract the contents of the zip file to a temporary location.
2. Locate the CD Developer folder and run the CD Browser.exe to begin the installation.

   The IC Install program performs the following checks:

   - Check that an existing copy of Agile Business Suite Developer or Agile Business Suite Runtime GCA version is installed.
   - Check if files which need to be updated are in use.
3. If the checks are successful, a dialog box appears which confirms that an existing version of the software exists. The existing version is upgraded prior to continuing with the installation of the IC.
4. Click **Yes** to continue, or **Cancel** to exit the installation.

5. If Agile Business Suite Runtime environment is also installed on the same computer as Developer, the IC for Developer changes the version numbers between the two products. Therefore you must upgrade the Runtime environment to the equivalent version after you have completed the Developer upgrade. A dialog box advises you of this requirement, and asks you to confirm that you wish to continue with the Developer upgrade.
6. Click **Yes** to continue, or **No** to exit the installation.

From this point, the installation proceeds in the same way as the base GCA release installation. Refer to Performing the Developer Installation for more information.

Installing Interim Corrections for Runtime for ClearPath MCP

Copying the Runtime Install Job from the Release Media

To copy the MCP Runtime install job from the release media, perform the following:

1. Obtain the release media and extract the IC container from its zip file to a temporary location.
2. Map a network drive to your privileged usercode on the MCP host.
3. Copy the container file to the MCP host.
4. Disconnect the network drive.
5. From CANDE, log in using the privileged usercode and unwrap the container file.

   ```
   WFL UNWRAP *= OUTOF <container file>
   TO <Transfer pack>(RESTRICTED=FALSE)
   ```

6. Download the installation WFL.

   ```
   COPY (TRANSFER)IC/90/<IC number>/NGEN30/WFL/RUNTIME
   AS NGEN30/WFL/RUNTIME
   FROM <Transfer pack>(PACK)
   ```

Installing the Authenticate File

The Authenticate file allows you to install an IC release to a new runtime environment without installing the GCA release first. Install the Authenticate file if you are installing an IC release to a new runtime environment.

To install the authentication file, run the following command:

```
WFL UNWRAP (TRANSFER)GCA/90/1000-<nn>/NGEN30/AUTHENTICATE
AS (<Runtime Usercode>)NGEN30/AUTHENTICATE
OUTOF <GCA container>
TO <Runtime pack>(RESTRICTED=FALSE)
```

Installing the MCP Runtime Software

To install the MCP Runtime software, perform the following:

1. Log in with privileged usercode.
2. Start the Runtime WFL by entering:

   ```
   START NGEN30/WFL/RUNTIME
   ("usercode","pack","aliaspack", media parameter)
   ```

The *usercode* value is the usercode to which the Runtime is installed, which might be an asterisk (*).

The *pack* value is the family name of the pack to which the Runtime is installed, which might be *DISK* or *altpack*.

The *aliaspack* value is the pack for your station alias file. Refer to the *Agile Business Suite Runtime for ClearPath MCP Administration Guide* for more information on station aliases.

media parameter = "MD=*MediaDirectory* MN=*MediaName* N=*Release#*"

MediaDirectory is the directory containing the installation files:

(TRANSFER)IC

MediaName is the name of the pack on which the installation files are located.

<Transfer pack>

Release# is the number from the release container file and has the format **nnnn-nn**.

<IC number>

For example:

```
START NGEN30/WFL/RUNTIME
("RTUSER", "RTPACK", "DISK",
"MD=(TRANSFER)ETA/IC MN=TFRPACK N=1001-01")
```

If the installation does not detect GCA release, you will be prompted with the following messages.

```
>>> (<usercode>)NGEN30/AUTHENTICATE ON <pack> IS MISSING OR INVALID <<<
COPY VALID AUTHENTICATE FILE FROM THE GCA RELEASE: AX TO CONTINUE OR DS
```

When the messages appear, perform the following:

1. Copy the valid authenticate file from the GCA release to (<usercode>/NGEN30/AUTHENTICATE ON <pack>) and respond with AX to continue with the installation.

   Refer to Installing the Authenticate File for instructions on retrieving the authenticate file.

2. Respond with DS to terminate the installation.

Note: *These messages cannot be translated because MLSLIBRARY has not been installed yet.*

Performing the First Application Build after Updating the Runtime

To improve application availability during the first deployment after an AB Suite IC update, the MCP Runtime deployment process has been enhanced to limit the occasions when an active application must be disabled for the duration of the first system deployment after an IC update.

For most IC updates, it is possible for the application to remain active during the first deployment after the IC update. After installing an IC for the MCP Runtime (and the associated Developer release), you can leave your application active while you do the next system build.

However, it is still necessary to use the Rebuild option with the first deployment of the system and reports after an IC update, and you must deploy all reports. This ensures code consistency across the application.

There are instances when it is necessary to have the system disabled for the duration of the first deployment, or to restart the system after the first deployment. The conditions that require the system to be disabled for the first deployment or to be restarted after the first deployment are described below.

Application Build Instructions

To deploy your application, perform the following steps:

1. As a part of pre-build preparation, remove your BuilderCache and BuilderOutput directories.
2. Start the deployment.
    a. Right-click the deployment folder and select **Rebuild** or **Folder Only Rebuild**.
    b. On the **Host Login** dialog boxer the login details.
    c. Click **OK**.
3. Respond to prompts and Build Log messages as recommended in the following topics.

LINCSUPPORT

If there is a change to LINCSUPPORT, the system must be disabled for the duration of the first deployment. This prevents duplicate LINCSUPPORT libraries in the mix for the application, which causes the system to hang.

After an IC has been installed, the first system deployment will check for a change to LINCSUPPORT and check whether the application is active. If there is a change to LINCSUPPORT and the application is active, the deployment will advise the user that the application must be disabled for the duration of the rest of the deployment. The deployment will not continue until the application has been disabled.

The following messages appear in the Build Log for a build or the Sumlog for a transfer:

```
"New LINCSUPPORT installed, you must disable your system to continue the deployment."
"PROGRAMMATICALLY SUSPENDED"
"<database> CONTROL FILE IN USE – WHEN DB CLOSED, OK TO CONTINUE"
```

Action required:

1. Disable the system.
2. Respond to the waiting entry.

ENVIRONMENT, LSS, and COMS_LINC_TP

The application might be active during the first deployment after the IC update. If there is a change to ENVIRONMENT, LSS, or COMSP_LINC_TP, the system must be restarted after the deployment. This activates the newly installed code files for these libraries.

After an IC has been installed, the first system deployment will check for a change to ENVIRONMENT, LSS, and COMS_LINC_TP and check whether the application is active. If there is a change to any of these libraries and the application is active, the deployment will include a log entry in the log for each of the changed libraries. (For builds, the message will be included in the Build Log. For transfers, the message will be in the Sumlog.) The log entry will advise the user that the application must be restarted after the deployment is complete.

The following messages might appear in the Build Log for a build or the Sumlog for a transfer.

```
"New LSS installed, RESTART application after this generate Job <job#>"
"New COMSTP installed, RESTART application after this generate Job <job#>"
"New ENVIRONMENT installed, RESTART application after this generate Job <job#>"
```

Action required:

1. Wait for the deployment to complete.
2. Restart the system immediately.

Recommendation:

If you choose to allow your application to remain active during the first deployment after an IC update and you do not normally review the Build Log or Sumlog afterwards, you should always restart your application after first deployment to ensure that the new libraries are activated.

LOGIC

If there is a change to LOGIC, the first system deployment after installing the IC must be a build with the Rebuild option. Having some code libraries with the old LOGIC and some code libraries with the new LOGIC would result in runtime issues.

After an IC is installed, the first system deployment checks for a change to LOGIC and then checks whether the deployment is using the Build or Rebuild option. If there is a change to LOGIC and the deployment is using the Build option, a message is logged in the Build Log. The message advises you to deploy your application with the Rebuild option. You must do this as soon as possible after the deployment is complete.

The following message appears in the Build Log:

```
"A new LOGIC is available. The application should be deployed with a REBUILD."
```

Action required:

1. Wait for the deployment to complete.
2. Deploy the system with the Rebuild option.

Recommendation:

The first system deployment after an IC update must be a build with the Rebuild option. This applies to the source system used in Runtime Transfers as well.

If you are performing the first deployment of the source system for the Runtime Transfer after an IC update and you see a message in the Build log, you must do another deployment with the Rebuild option before you perform the transfer to deploy the target system.

REPORT_INFO

If there is a change to REPORT_INFO, the first report deployment after installing the IC must include all reports. (If it is not possible to deploy all the reports at once, deploy the critical online reports first, and then the batch reports.)

After an IC is installed, the first report deployment checks for a change to REPORT_INFO and then checks whether the report deployment is using the Rebuild option. If there is a change to REPORT_INFO and the report deployment is not a Rebuild, a message is logged in the Build Log. The message inform you that REPORT_INFO has changed.

The following message appears in the Build Log.

```
“New REPORT DUMPINFO is available, all reports require a REBUILD”
```

Action required:

1. Wait for the deployment to complete.
2. Deploy all reports with the Rebuild option.

Recommendation:

The first report deployment after an IC update must be a build with the Rebuild option. This applies to the source application used in Runtime Transfers as well.

If you are performing the first deployment of the source application for the Runtime Transfer after an IC update and you see the message in the Build log, you must perform another deployment with the Rebuild option before you perform the transfer to deploy the target system.

If you see the message in the Build log and have included all the reports within a system build, perform another report build with the Rebuild option only if the last report build was done with the Build option.

3826 5815-009