



DocuSign Signature Appliance Administrator Guide

Copyright ©2003-2016 DocuSign, Inc. All rights reserved.

For information about DocuSign trademarks, copyrights and patents refer to the [DocuSign Intellectual Property page](https://www.docusign.com/IP) (<https://www.docusign.com/IP>) on the DocuSign website. All other trademarks and registered trademarks are the property of their respective holders.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of DocuSign, Inc. Under the law, reproducing includes translating into another language or format. Every effort has been made to ensure that the information in this manual is accurate. DocuSign, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

DocuSign Signature Appliance Administrator Guide, version 8

If you have any comments or feedback on our documentation, please send them to us at: Documentation@DocuSign.com.

Table of Contents

Chapter 1: Overview	9
Requirements for Data Authentication Systems	9
Introduction to DocuSign Signature Appliance	9
<i>Environments Supported by DocuSign Signature Appliance</i>	10
<i>Applications that Work with DocuSign Signature Appliance</i>	10
<i>DocuSign Signature Appliance Components</i>	11
DocuSign Signature Appliance Guides	11
DocuSign Signature Appliance Hardware Models	12
End User Platforms.....	12
Intended Audience.....	12
Chapter 2: DocuSign Signature Appliance Architecture and Data Flow	13
Enrollment Using a Standard User Management Application	13
Central Storage of Signing Keys	14
User Authentication.....	14
Extending User Authentication.....	14
Turnkey Solution.....	15
Directory Independent Environment.....	15
Using DocuSign Signature Appliance’s Internal CA	15
Using DocuSign Signature Appliance in Manual External CA Mode.....	16
Using DocuSign Signature Appliance in Automatic External CA Mode	16
Using DocuSign Signature Appliance in Common Criteria EAL4+ Deployments	17
<i>Extended Authentication using an External Radius Server</i>	17
<i>User Activation</i>	18
<i>Signature key Generation and Certificate Enrollment</i>	19
<i>Physical Security: Tamper Evidence and Tamper Response</i>	19
<i>Recommended OTP Devices</i>	20
Using SAML Tickets to Authenticate Users	20
<i>ADFS Flow</i>	21
<i>Passive Mode using the Web App and Connector for SharePoint</i>	21
<i>Active Mode Using the DocuSign Signature Appliance Client</i>	22
<i>SAML Ticket Requirements</i>	22
Chapter 3: Installing DocuSign Signature Appliance	23
Installing the Administrative Client	23
<i>Installation Requirements</i>	24

<i>Installing the Administrative Client</i>	24
<i>Uninstalling the Administrative Client</i>	25
Installing the DocuSign Signature Appliance Hardware version 8.0	25
Installing the DocuSign Signature Appliance Central FIPS Appliance Hardware 8.0	26
<i>To install the DocuSign Signature Appliance Central FIPS v8.0 appliance hardware:</i>	27
Installing the CoSign Appliance Hardware version 7.0	30
<i>Installing the CoSign Central FIPS Appliance Hardware version 7.0</i>	30
<i>To install the CoSign Central FIPS appliance hardware:</i>	31
<i>Installing the CoSign Central Enterprise Appliance Hardware v7.0 and 8.0</i>	33
<i>To install the DocuSign Signature Appliance Central Enterprise appliance hardware:</i>	34
Installing the Appliance Software	35
<i>Installing DocuSign Signature Appliance in a Microsoft Active Directory Environment</i>	36
<i>Installing DocuSign Signature Appliance in an LDAP based Environment</i>	48
<i>Installing DocuSign Signature Appliance in a Directory Independent Environment</i>	54
<i>Installing DocuSign Signature Appliance in a Common Criteria EAL4+ Mode as a Signature Creation Device or Seal Creation Device</i>	59
<i>Installing an Internal Certificate Authority</i>	61
<i>Using an External CA in Manual Mode</i>	65
<i>Using an External World Wide Verifiable CA in Automated Mode</i>	66
<i>Installing DocuSign Signature Appliance as a Subordinate CA</i>	67
<i>Multi-Language Support</i>	70
Chapter 4: Deploying the DocuSign Signature Appliance Client	71
Deploying the Client.....	71
<i>Deployment Options</i>	71
<i>Installing the DocuSign Signature Appliance Client</i>	72
<i>Uninstalling the DocuSign Signature Appliance Client</i>	76
<i>Distributing DocuSign Signature Appliance Information through the SCP</i>	76
Using the Control Panel	78
<i>User Actions</i>	79
<i>Administrator Actions</i>	79
<i>CoSign Control Panel Menu Bar</i>	79
<i>Control Panel – Tray Item</i>	80
<i>Directory Independent Environment Options</i>	80
Using the Graphical Signature Management Application	83
<i>Installing the Graphical Signature Capture Device</i>	84
<i>Managing Graphical Signatures</i>	85

<i>Creating an Image-Based Graphical Signature</i>	88
<i>Creating a Text-Based Graphical Signature</i>	90
Installing the Root Certificate and CoSign Verifier.....	92
<i>Adding the ROOT Certificate to a Trusted CA List (Active Directory only)</i>	92
<i>Using CoSign Verifier for Validation Purposes</i>	92
Extended Authentication Modes.....	92
Chapter 5: Managing the DocuSign Signature Appliance	94
Prerequisites to Using the Administration MMC	94
Starting the Administration MMC.....	94
<i>Administration MMC Capabilities</i>	95
Backing up the DocuSign Signature Appliance Data.....	96
Upgrading	97
<i>Upgrading to Version 7.1</i>	97
<i>Upgrading to Version 7.4</i>	98
<i>Upgrading to Version 7.5</i>	98
<i>Upgrading to Version 8.0</i>	98
<i>Uploading a Software Update</i>	98
Synchronizing DocuSign Signature Appliance with the Directory Service	99
Synchronizing DocuSign Signature Appliance with the External CA in Automated mode.....	100
Refreshing Certificates.....	101
Clearing CA files	101
Downloading Log Files.....	101
Shutting Down and Restarting DocuSign Signature Appliance Services	103
Restarting the Appliance	103
High Availability	103
Renewing the Subordinate CA Certificate	104
Uploading an SSL Certificate	106
Monitoring Performance Parameters of the Appliance	107
<i>Activating Performance Monitoring</i>	107
<i>Stopping Performance Monitoring</i>	107
<i>Viewing Performance Parameters</i>	107
Obtaining a New License	108
<i>Requesting a New License</i>	108
<i>Uploading the New License</i>	108
Changing System Parameters	109

<i>Users Directory Parameters</i>	110
<i>Key Management Parameters</i>	112
<i>Certificate Management Parameters</i>	112
<i>Client Security Setting Parameters</i>	116
<i>Auditing and Accounting Parameters</i>	117
<i>Alerts and Notifications Parameters</i>	117
<i>Password Policy</i>	118
<i>LDAP</i>	119
<i>Advanced Parameters</i>	120
<i>Extended Authentication</i>	122
<i>SNMP</i>	126
<i>SAML</i>	126
Restoring the Appliance	128
<i>Restoring the Appliance in Microsoft Active Directory</i>	128
<i>Restoring the Appliance in an LDAP Environment</i>	129
<i>Restoring the Appliance in a Directory Independent Environment</i>	129
Using the Users Management Utility	130
<i>Activating the Users Management Utility</i>	131
<i>Users Management Main Window</i>	131
<i>Users Management Menus</i>	133
<i>Users Management Toolbar</i>	140
Using Command Line Utilities	141
<i>GetBackup</i>	142
<i>GetEvt</i>	143
<i>restartServer.exe</i>	143
<i>Switch2Prim.exe</i>	144
<i>SetSCP</i>	145
<i>Groups</i>	145
Chapter 6: Using the Consoles	147
Console Types	147
<i>Overview of the Web-based Console for Hardware v8.0</i>	147
<i>Overview of the Built-in Console for Hardware versions prior to v8.0</i>	147
Using the Built-in Console –Hardware versions prior to 8.0	149
<i>Displaying Status</i>	149
<i>Enabling DHCP</i>	151

<i>Using a Static IP Address</i>	151
<i>Resetting the Tamper Mechanism (Enterprise Only)</i>	152
<i>Restoring Factory Settings</i>	153
<i>Shutting Down</i>	154
<i>Setting Time</i>	154
Using the Web-based Console	155
<i>Setting the Appliance IP Address</i>	156
<i>Setting Time</i>	157
<i>Shutting Down</i>	159
<i>Restarting the Appliance</i>	159
<i>Resetting the Tamper Mechanism</i>	159
<i>Restoring Factory Settings</i>	160
<i>Displaying Appliance Status</i>	161
Using the Touch Screen of a DocuSign Signature v8.0 Appliance	164
Restoring the Appliance After an Internal Hard Disk Failure.....	164
<i>In CoSign Hardware V7.0</i>	164
<i>In DocuSign Signature Appliance Hardware V8.0</i>	165
Chapter 7: Configuring High Availability.....	167
Overview of High Availability	167
Installing Appliances in a High Availability Configuration.....	168
<i>Installing the Primary DocuSign Signature Appliance</i>	168
<i>Installing an Alternate DocuSign Signature Appliance</i>	168
Managing the Alternate Appliance	172
Managing Data Replication in the Alternate Appliance.....	172
<i>Viewing Replication Status of an Alternate Appliance</i>	173
<i>Re-initializing an Alternate Appliance</i>	173
<i>Unsubscribing an Alternate Appliance</i>	174
Managing Primary Appliance Failure and Recovery.....	174
<i>Setting an Alternate Appliance to be the Primary Appliance</i>	174
<i>Setting a Previous Primary Appliance to be an Alternate Appliance</i>	176
Resubscribing an Alternate Appliance with a Primary Appliance.....	177
Upgrading Appliances Participating in a High Availability Cluster.....	177
Chapter 8: Configuration Utility	179
Overview.....	179
Using the Configuration Utility.....	179

<i>Configuration Utility Menus</i>	181
Running the Configuration Utility in Admin Mode	183
<i>Configuration File Operations</i>	184
<i>Group Policies Operations</i>	185
Running the Configuration Utility in End User Mode.....	185
Distributing the Client Configuration.....	186
<i>Distributing the Configuration Using Configuration Files</i>	186
<i>Distributing the Configuration Using Group Policy</i>	187
Setting Admin Configuration	187
<i>Admin – Appliance Installation</i>	187
<i>Admin – Performance Monitoring</i>	189
Chapter 9: Troubleshooting	190
Installation Problems.....	190
<i>IP Address is Invalid</i>	190
<i>Error When Setting the IP Address Via the Console Interface</i>	190
<i>Default Values Do Not Appear in the Directory Setup Dialog Box</i>	191
<i>The Appliance is Not in Factory Settings Mode</i>	191
<i>Installation Failed</i>	191
<i>Progress Bar Stops Advancing</i>	192
<i>Appliance Installation Issues</i>	192
<i>High Availability/Load Balancing – Alternate Installation</i>	192
Appliance Problems	192
<i>Appliance Does Not Start</i>	192
Console Problems	193
Client-Related Problems	193
<i>Cannot Enable the “Add Digital Signature to Outgoing Messages” Checkbox in Outlook</i>	193
<i>Cannot See Any Certificates in Store</i>	193
Administrative Problems	194
<i>System Parameters Do Not Appear in the Administration MMC</i>	194
<i>All Administration MMC Operations Fail</i>	194
<i>System Does Not Respond</i>	194
<i>New Users Do Not Receive Certificates</i>	195
<i>Restore Appliance Fails</i>	195
<i>Backup Operation Fails</i>	196
Appendix A: Installation with Reduced Privileges.....	197

Overview.....	197
Regular Installation	198
<i>Creating a New Computer Account for the Appliance.....</i>	<i>198</i>
<i>Joining the Appliance to MS Domain</i>	<i>198</i>
<i>Creating a Services Connection Point (SCP)</i>	<i>198</i>
<i>User Synchronization.....</i>	<i>198</i>
<i>Updating the userCertificate Attribute for Users.....</i>	<i>198</i>
<i>CA Root Certificate Information.....</i>	<i>198</i>
<i>CA CDP (Certificate Distribution Point).....</i>	<i>199</i>
Installation with Reduced Privileges.....	199
<i>Preliminary Action – Adding the Computer to the Domain.....</i>	<i>199</i>
<i>Installing in a Reduced Privileges Environment.....</i>	<i>200</i>
<i>Complementing the Installation with Missing Capabilities</i>	<i>201</i>
Appendix B: Centralized Client Installation	204
Automatic Client Deployment using Microsoft SCCM.....	204
Installation Components	204
Defining and Advertising a Client Task Sequence.....	205
<i>Step 1: Define Packages.....</i>	<i>205</i>
<i>Step 2: Create a Task Sequence</i>	<i>205</i>
<i>Step 3 – Advertise the Task Sequence</i>	<i>212</i>
Index	213

Chapter 1: Overview

Over the last four decades, the biggest challenge of IT departments in many organizations was moving to a paperless work environment. Seemingly, there was tremendous success in this regard. Today, most transactions in the business world are performed electronically:

- Documents are written using word processing programs.
- Messages are sent via email.
- Inventories and purchases are tracked using Enterprise Resource Planning (ERP) systems.
- Medical information is stored in Electronic Medical Record (EMR) systems.

Although these transactions are performed in a paperless environment, organizations have still not managed to find an easy way to get rid of the paper used for data authentication (signing the authenticity of the data). Today, although organizations have invested large amounts of funds and other resources in creating paperless environments, their workers are still printing every transaction, signing it, and saving the printed copy. These organizations require a digital method for data authentication.

By moving to a viable electronic data authentication system, organizations can reduce their printing, archiving, shipping, and handling costs. In addition, better and more competitive customer service can often be provided.

Requirements for Data Authentication Systems

A viable data authentication system must meet the following specifications:

- *Security* – The system must ensure that no one other than the data creator can tamper with or change the data in any way.
- *Third-party validation* – The system must enable any third party to validate the authenticity of the data. If a dispute arises between the parties (the data creator and recipient), any third party must be able to validate the data authenticity in order to settle the dispute.
- *System independence* – Data authentication must be independent of the system that created the data. Users must be able to validate the authenticity of the data using a known standard that is independent of any specific system.
- *Validation over time* – Users must be able to validate data authenticity at any point in time. Authenticity cannot expire at any point.

Currently, the only data authentication method known to support all of these requirements is the Public Key Infrastructure (PKI) method of authenticating data, simply called “digital signatures”.

Introduction to DocuSign Signature Appliance

DocuSign Signature Appliance is a PKI-based, off-the-shelf digital-signature solution that can be integrated with a wide range of applications. In this way, DocuSign Signature Appliance enables organizations to embed digital signatures in various documents, forms, and transactions. DocuSign Signature Appliance is a turnkey, hardware-based solution that is easily and quickly deployed in the network and provides cost-effective digital-signature capabilities for the organization.

DocuSign Signature Appliance includes all the components needed for PKI-based digital-signature deployment. You do not need to install any other device or integrate any other component for the system to work.

Environments Supported by DocuSign Signature Appliance

DocuSign Signature Appliance integrates with leading user management systems, including Microsoft Active Directory and a variety of LDAP (Lightweight Directory Access Protocol) based directories, such as IBM Tivoli. This integration ensures no overhead in managing the digital-signature system and signature credentials (i.e., the private keys that are needed in a PKI environment), solving one of the main problems of legacy digital-signature systems. System managers, network managers, and end-users can continue to use the IT infrastructure in the same manner as before DocuSign Signature Appliance was installed.

DocuSign Signature Appliance stores the signature credentials in a secure server, ensuring that the signer has exclusive access to his or her signature credentials, while still maintaining a centrally managed solution. This is necessary in order to fulfill the security requirement of the data authentication system.

Applications that Work with DocuSign Signature Appliance

An increasing number of applications can work with DocuSign Signature Appliance as their digital-signature layer without needing any further integration, including:

- Microsoft Office 2010/2013/2016 (Word, Excel, and PowerPoint)
- Microsoft InfoPath 2010/2013
- Adobe Acrobat
- Microsoft SharePoint 2010/2013
- XML
- TIFF files
- Word Perfect
- Microsoft Outlook and Outlook Express
- Adobe Server forms (for signing web forms)
- AutoCAD
- Lotus Notes
- Microsoft BizTalk
- FileNet eForms
- Verity Liquid Office
- ERP systems (e.g., SAP)
- OpenText
- Oracle
- Crystal Reports
- Web applications

- Any application that has a *print* option can use DocuSign Signature Appliance to generate a PDF file and sign it.

For information on using DocuSign Signature Appliance with other applications, contact DocuSign technical support.

DocuSign Signature Appliance Components

DocuSign Signature Appliance includes the following components:

- **DocuSign Signature Appliance** – The DocuSign Signature Appliance hardware and software, connected to the organization’s network. For more information, refer to [Chapter 3: Installing DocuSign Signature Appliance](#).
The DocuSign Signature Appliance can be interfaced either through installed client software or through a Web Services interface that can be based on either a SOAP or RESTful API.
- **Client** – The DocuSign Signature Appliance Client software, installed on the users’ computers. For more information, refer to [Chapter 4: Deploying the DocuSign Signature Appliance Client](#).
- **Administrator** – The DocuSign Signature Appliance Administrative software that includes the Microsoft Management Console (MMC) snap-in, installed on the administrative computer. For more information, refer to [Chapter 5: Managing the DocuSign Signature Appliance](#).
- **Connector for SharePoint** – This connector enables adding digital signature functionality to documents managed by Microsoft SharePoint, or using digital signatures within any workflow procedure that is based on Microsoft SharePoint.
- **Web App** – This application is deployed in the Microsoft Web Server of the organization and enables users to sign documents without installing any client component. Web App can use the local DocuSign Signature Appliance for performing digital signature operations. Applications can interact with the Web App and add a digital signature to documents using a web based interface.
- **Mobile App** – This mobile application, which can be installed on Android-based devices or Apple iOS devices, enable users to sign documents using their mobile devices.
The mobile devices interface directly with the DocuSign Signature Appliance via a RESTful interface.
The Mobile App can interface with either the organizational DocuSign Signature Appliance, or trial system.
- **DocuSign Signature Appliance Signature APIs** – Developers can use local and network APIs to integrate their applications with DocuSign Signature Appliance Central appliances.

DocuSign Signature Appliance Guides

DocuSign Signature Appliance documentation includes the following guides:

- *DocuSign Signature Appliance Administrator Guide* – Provides all the information necessary for an administrator to install and manage the DocuSign Signature Appliance in the various environments.
- *DocuSign Signature Appliance Client User Guide* – Provides all the information necessary for an end user to use DocuSign Signature Appliance. Includes information about special add-ins for various applications such as Microsoft Office.

- *DocuSign Signature Appliance Signature APIs Developer's Guide* – Provides all the information necessary for a developer to integrate their application with DocuSign Signature Appliance.

DocuSign Signature Appliance Hardware Models

There are several available hardware models of the DocuSign Signature Appliance. All the models are easy-to-deploy and easy-to-use digital-signature appliances that integrate with leading applications. They enable organizations to embed digital signatures that can include a graphical (handwritten) signature. The models differ in functionality, as follows:

- *DocuSign Signature Appliance Central Enterprise* – This is the most commonly used DocuSign Signature Appliance. The hardware is based on a rack-mountable 1U box packaged in a standard commercial casing.
- *DocuSign Signature Appliance Central FIPS* – This 3U rack-mountable box is based on a sealed, tamper-response casing. The hardware box is FIPS 140-2 level 3 certified. This model is also used for deploying DocuSign Signature Appliance in Common Criteria EAL4+ deployments. Starting from DocuSign Signature Appliance version 8, a new version 8 hardware model is available. The new hardware version has some functionality changes.

Note: Throughout this manual, the term “DocuSign Signature Appliance” refers to all hardware models (Enterprise and FIPS) and hardware versions, unless stated otherwise.

End User Platforms

DocuSign Signature Appliance supports various end-user platforms for signing documents or data.

- **Desktop applications** – Desktop applications interact with the DocuSign Signature Appliance through the installation of the Client. For example, end users can sign using OmniSign, a desktop application that enables users to sign PDF files.
- **Web applications** – Web applications do not require the end user to install any software; instead, the end user signs documents and data through a web portal or web application. Web applications offered are:
 - ◆ Microsoft SharePoint integrated with Connector for SharePoint, enabling the end user to sign documents or data stored inside SharePoint.
 - ◆ The Web App which can be installed in the organizational portal. The end user can view the document via the web interface and visibly sign the document as part of the web interface.
- **Mobile Applications** – The Mobile App enable end users to sign documents using their mobile devices. The Mobile App can be installed either on Android devices or iOS devices. The Mobile App currently supports signing of PDF files: the PDF file is loaded into the application, and the user can view the entire document and sign it.

Intended Audience

This guide is intended for developers wishing to integrate digital signatures into their system.

Chapter 2: DocuSign Signature Appliance Architecture and Data Flow

DocuSign Signature Appliance is a hardware appliance that is installed on the network. The appliance includes all the necessary components for PKI-based digital signatures. The appliance integrates with the organization's user management system to eliminate overhead associated with managing users in a digital-signature system.

To prevent a malicious user from signing with the credentials of a user whose desktop was left running, user authentication is performed by either the signing application or the desktop operating system. Once a user is authenticated, DocuSign Signature Appliance signs all of the user's signing requests using the user's signing credentials.

[Figure 1](#) illustrates the DocuSign Signature Appliance architecture.

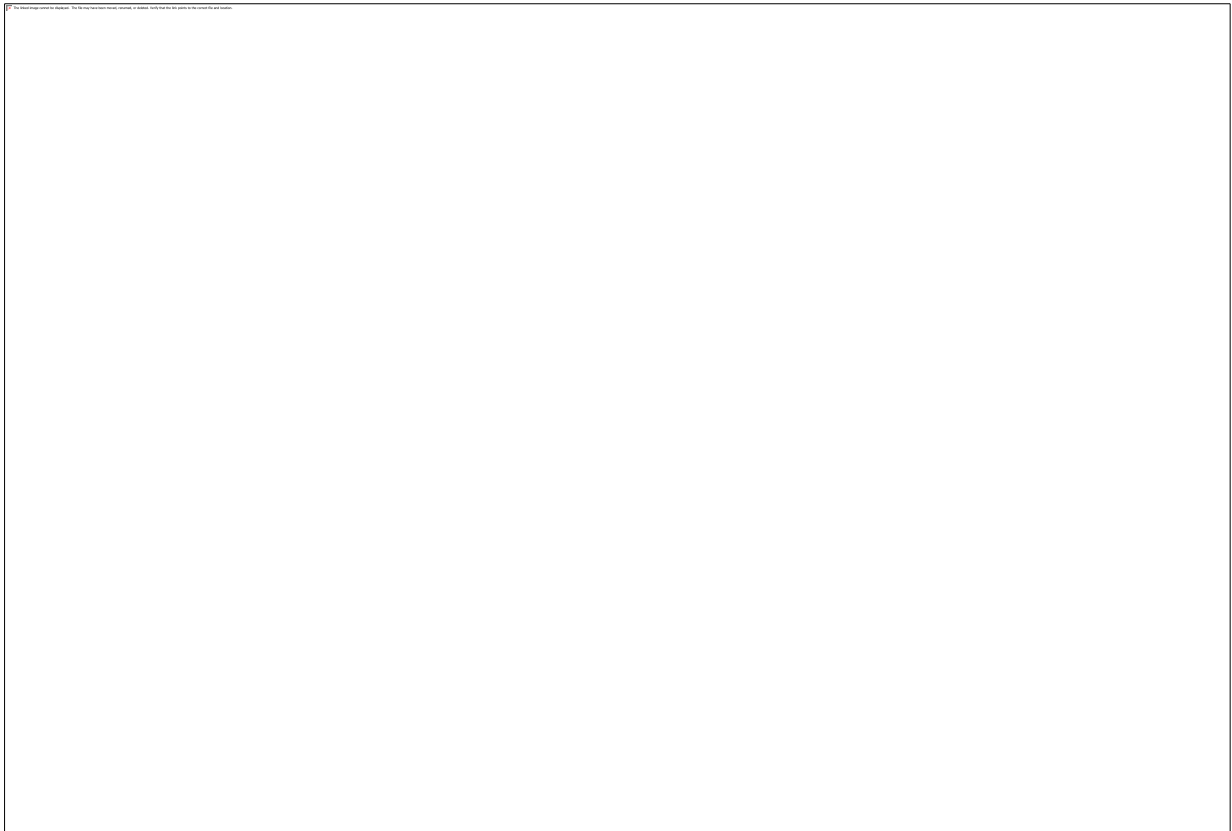


Figure 1 Appliance Architecture

Enrollment Using a Standard User Management Application

With DocuSign Signature Appliance, enrollment in the digital-signature system (i.e., creating the signature credentials) is performed automatically when a new user joins the system, using one of the supported user management systems.

A user's signature credentials are renewed automatically if the user is part of the system at the yearly renewal time. Once a user is removed from the users list (for example, upon leaving the organization), the user's signature credentials are revoked and the user can no longer perform a digital signature operation.

This enables DocuSign Signature Appliance to eliminate the costs associated with managing users in two systems, both in the regular user management system and in the digital-signature system.

Central Storage of Signing Keys

In traditional PKI systems, users can choose to store their signing keys in personal software or hardware tokens. This creates many management problems and significantly increases the system's Total Cost of Ownership (TCO). In DocuSign Signature Appliance, the signature credentials are stored in a central, secure repository.

The following are several advantages of this scheme:

- Users have access to their signature credentials from any computer they are working with, without having to import or export signature credentials.
- There is no need for distributing signature credentials since all credentials are centrally managed.
- There is no need for issuing temporary credentials or handling forgotten tokens.
- Signature credentials cannot be lost or stolen.

With DocuSign Signature Appliance's central, secure repository, the security level is not affected. The repository is like a huge collection of network-attached virtual SmartCards that combine with the organization's user management and authentication system.

User Authentication

In the DocuSign Signature Appliance environment, user authentication can be performed using the same authentication method as was used by the organization prior to the installation of the DocuSign Signature Appliance. If the organization has chosen to use a certain authentication method, such as a user password, this method will also be used when performing digital signature operations.

Once a user is authenticated, the following data flow illustrates how documents are digitally signed:

1. In a paperless environment, a user requires a digital signature.
2. The user's application sends a request to DocuSign Signature Appliance with the user's credentials (in the case of Microsoft Active Directory, credentials are sent automatically).
3. DocuSign Signature Appliance finds the correct signing key for the user and signs the document with this key.
4. DocuSign Signature Appliance returns the signature to the requesting application.

Extending User Authentication

You can configure DocuSign Signature Appliance to prompt the end user for credentials upon every digital signature attempt. This functionality provides a solution for organizations that would like to enhance the security of the digital signature operation, beyond using a regular user ID and password. If authentication is successful, DocuSign Signature Appliance allows accessing the user's key and performing the digital signature operation.

The following mechanisms can be used as part of extended user authentication:

- *One Time Password (OTP)* – The user uses an OTP mechanism such as a Yubiko token. In this mechanism the password is based either on a password that is changed every several seconds or on a button that is pressed by the end user.
In these types of deployments, a dedicated Radius Server that is deployed in the organizational network is used for validating the OTP entered by the signing user.
This mode is mandatory when DocuSign Signature Appliance is deployed in Common Criteria EAL4+ certified environments as a Qualified Signature Creation Device.
It is important to note that OTP devices or OTP related information should be delivered in a secure manner to end users.
- *SmartCard* – The user uses a SmartCard for authentication.
- *Biometric Device* – The user uses a biometric device for authentication.

Turnkey Solution

DocuSign Signature Appliance provides a complete and integrated digital-signature system. DocuSign Signature Appliance integrates the different components required by a digital-signature system along with a graphical signature capture mechanism. Since DocuSign Signature Appliance uses the organization's existing user management system, no extra overhead is needed to manage the users in the digital-signature system. In addition, DocuSign Signature Appliance easily integrates with many of the leading applications that are digital-signature enabled, such as Microsoft Word and Adobe Acrobat, without requiring any additional development.

Directory Independent Environment

DocuSign Signature Appliance can also be used by organizations that maintain their own proprietary user-management system.

When DocuSign Signature Appliance is installed in a Directory Independent environment, the organization's administrator can either use DocuSign Signature Appliance's users management utility or an application developed by the organization to create users and consequently generate keys and certificates for the new users.

These users are just like users in a Microsoft Active Directory environment or LDAP environment, and they can use digital signature enabled applications such as Microsoft Word and Adobe Acrobat to perform digital signature operations.

A Directory Independent environment can also be used by organizations that do not have a user directory that is supported by DocuSign Signature Appliance (currently, Microsoft Active Directory or LDAP-based directory). DocuSign Signature Appliance enables these organizations to manage the users through GUI-based user management utilities.

Using DocuSign Signature Appliance's Internal CA

DocuSign Signature Appliance can be installed with an internal CA. The internal CA is initiated during installation and a new CA ROOT key is generated. For every new signer, DocuSign Signature Appliance generates a new key and the internal CA generates a certificate for the key. When the signer's account is deleted, the signature key is deleted and the user's certificate is revoked. In addition, if certain user attributes (such as user name or email address) are changed, a new certificate is automatically issued for the user.

The user's certificate is valid for a year and includes basic attributes necessary for performing a digital signature operation. This certificate will be automatically renewed close to its expiration date.

If a CA system is already installed within the enterprise, it is possible to have the DocuSign Signature Appliance's internal CA certificate certified by the organization's CA, thus DocuSign Signature Appliance acts as a subordinate CA.

Using DocuSign Signature Appliance in Manual External CA Mode

DocuSign Signature Appliance can be installed in a manual external CA mode, in which each end user is allocated an empty account, and must manually enroll for a certificate from an external CA. Certificate enrollment for each user is performed using an external certificate enrollment or RA application software. This application software uses standard Cryptographic APIs to access DocuSign Signature Appliance, and is not part of the DocuSign Signature Appliance solution.

When DocuSign Signature Appliance is installed in manual external CA mode, DocuSign Signature Appliance does not install its internal CA, so users are not automatically provided with a certificate. During the enrollment:

- The enrollment application software requests that the DocuSign Signature Appliance generate a new signature key for the specific user. The key is generated within the DocuSign Signature Appliance and under the specific user account in a non-extractable manner.
- A certificate request is sent to the external CA.
- The external CA issues an X-509 certificate and sends it back to the enrollment application software.
- The enrollment application software uploads the certificate to the user's account.

The user is now ready to sign with the newly-enrolled certificate.

Several signature keys and certificates can be created and stored for any given user, depending on the organization's needs.

The main drawback of this mode of work is that it requires manual enrollment for each user. Manual enrollment requires user intervention, as well as substantial management time and effort. Manual enrollment also requires additional efforts spent on certificate renewal and certificate revocation. However, there are cases where you must employ manual enrollment. These include:

- Cases where it is required that the certificate be provided by a qualified CA of a certain country or the EU.
- Cases where the certificate must have specific or specialized attributes not provided by the built-in CA.
- Cases where the certificate must be provided by a World Wide verifiable CA that is not currently supported by the automatic external CA. In this case, the verifying party's PC is already installed with the ROOT certificate, so the verifying party does not have to manually install a ROOT certificate. This makes documentation validation easier.

Using DocuSign Signature Appliance in Automatic External CA Mode

An alternative external certification mode is available that addresses the deficiencies of the manual external certificate enrollment process described above.

In Automatic external certification mode, the DocuSign Signature Appliance automatically interfaces with the external CA during the process of generating a single signature key and certificate for each user. The user's certificate is automatically renewed close to its expiration. In addition, if the user account is revoked, the user's certificate is also automatically revoked.

All communication between the DocuSign Signature Appliance and the external CA is secured based on the HTTPS protocol. Note that using this mode requires an outbound network connection from the DocuSign Signature Appliance to the Internet.

The Comodo certificate authority can optionally be used for this purpose. The certificate authority that will serve as the Automatic External CA is selected during the DocuSign Signature Appliance installation process.

Using DocuSign Signature Appliance in Common Criteria EAL4+ Deployments

The DocuSign Signature Appliance FIPS appliance can be deployed in a Common Criteria EAL4+ mode. In this type of deployment, additional security measures should be carried out in the environment of the DocuSign Signature Appliance to ensure the appliance and its environment are protected from both physical and logical threats.

In Common Criteria EAL4+ deployments DocuSign Signature Appliance is installed in Directory Independent mode. This means that the DocuSign Signature Appliance is not synchronized with any external users directory.

In the future DocuSign Signature Appliance version 8.2, it will be possible to install DocuSign Signature Appliance in either of the following modes:

- Common Criteria mode as a Signature Creation Device – In this mode, the end user is authenticated based on two factor authentication (i.e., providing a Static Password and an OTP).
- Common Criteria mode as a Seal Creation Device – In this mode, the end user is authenticated based on one factor authentication (i.e., providing a Static Password).

Extended Authentication using an External Radius Server

In a Common Criteria EAL4+ deployment when DocuSign Signature Appliance is deployed as a Signature Creation Device, all digital signature operations require extended authentication, as described in [Extending User Authentication](#).

Specifically, the user is requested to enter a fixed password as well as a one-time-password (OTP) using a personal OTP device provided by the organization. The fixed password and OTP are validated upon any digital signature operation request and only when the validation is successful does the DocuSign Signature Appliance continue with the digital signature operation.

As part of DocuSign Signature Appliance deployment in Common Criteria EAL4+ mode, the actual OTP validation is performed in the DocuSign Signature Appliance. Special software must be integrated with the deployed Radius Server software to enable OTP validation by the DocuSign Signature Appliance firmware. Any information required for the purpose of OTP validation is sent securely (via SSL/TLS) to the DocuSign Signature Appliance.

For more information on how to integrate the functionality into the Radius Server, contact ARX.

The Radius Server should be installed and configured so that DocuSign Signature Appliance will interface the Radius Server using a Radius Protocol, and the Radius Server will access the DocuSign Signature Appliance using the secured protocol.

Always make sure that:

- Only a dedicated administrator of the organization performs the following:
 - ◆ Installs the Radius software and the component that accesses the DocuSign Signature Appliance.
 - ◆ Performs any technical configuration of the Radius software.
 - ◆ Installs and maintains any additional software in the Radius Server.
- The Radius Server is fully observed and can be accessed only by authorized personnel.
- The Radius Server limits network access to its resources.

OTP Management in the Radius Server

The Radius Server manages the following information, which must be kept securely by the Radius Server and protected with data integrity mechanisms:

- Information related to every OTP device used by end users. This information is mandatory for proper validation of the OTP, which is performed by the DocuSign Signature Appliance.
- Information that binds actual users with their specific OTP device, when applicable.

The following guidelines should be strictly followed. Any attempt to modify the guidelines may jeopardize the security of the DocuSign Signature Appliance system:

- Only an authorized and dedicated administrator can manage users, OTP devices, and OTP device information in the Radius Server. The administrator's responsibilities include:
 - ◆ Adding, updating and deleting users in the Radius Server.
 - ◆ Uploading information for batches of OTP devices, when applicable.
 - ◆ Uploading OTP device information.
 - ◆ Binding an OTP device or OTO device information to a user.
- The authorized and dedicated administrator assigns OTP devices to end users via the Radius Server, with the following restrictions:
 - ◆ If OTP devices are distributed to end users, they should be distributed in a secure manner.
 - ◆ If OTP device information is distributed to end users, it should be distributed in a secure manner.
 - ◆ If a user is revoked in the DocuSign Signature Appliance, the user's OTP device should be revoked too and should not be allocated to a different user.
 - ◆ A specific OTP device or specific OTP device information may not be bound to several users.
 - ◆ A user's OTP device may not be replaced once the user account is activated. To replace an OTP device, the user account must first be revoked and a new account created.

User Activation

When the DocuSign Signature Appliance is running in Common Criteria EAL4+ mode, a user activation process is required for every new user created. Without activation, no operation can be performed by the

user.

Activation is required also when DocuSign Signature Appliance is deployed in Common Criteria EAL4+ mode as a Seal Creation Device.

Every new user receives a fixed activation password in addition to the OTP device mentioned above. The activation password must be delivered in a secure manner.

Note that an OTP device is not required if DocuSign Signature Appliance is installed as a Seal Creation Device.

The new user uses the DocuSign Signature Appliance client to perform the activation process. During the activation process, the user is required to enter his/her activation password, new fixed password, and the OTP (if required). The activation process can be performed only once per user account.

It is important to note that if a new user receives a message that the account has already been activated, this may indicate that the user account was compromised and the issue should be investigated by the organization.

Signature key Generation and Certificate Enrollment

In Common Criteria EAL4+ installations, DocuSign Signature Appliance is installed without an internal CA. This means that all users' keys and certificates are created as part of a user enrollment process using an external CA. For more information, refer to [Using DocuSign Signature Appliance in Manual External CA Mode](#).

The end user must use the Certificate Authority's tools or trusted third party tools that are installed in the same PC as the DocuSign Signature Appliance client is installed.

These tools can use either the DocuSign Signature Appliance API (DocuSign Signature Appliance Signature Local API or DocuSign Signature Appliance Signature API) or other APIs to interface with the DocuSign Signature Appliance for the purpose of generating a signature key for the user in his/her account and generating a certificate request for the user. The certificate request is sent by these third party tools to the Certificate Authority.

The Certificate Authority sends the certificate to the end user, who loads it into the DocuSign Signature Appliance via a DocuSign Signature Appliance API (DocuSign Signature Appliance Signature Local API or DocuSign Signature Appliance Signature API) or other APIs (such as PKCS#11, Microsoft CAPI or JAVA JCA interface), which are offered by the DocuSign Signature Appliance Client software.

Physical Security: Tamper Evidence and Tamper Response

DocuSign Signature Appliance is encased within a tamper-responsive and tamper-evident steel box. All the DocuSign Signature Appliance vents are baffled so it is not possible to view any of the internal hardware components. It is also not possible to probe any of the DocuSign Signature Appliance internal hardware components.

The DocuSign Signature Appliance includes a removable cover. This cover is rigged with micro-switches, which are connected to an internal Tamper Device. When the tamper device is triggered, the appliance is immediately powered off. The mechanism works as follows:

Two of the screws holding the removable top case in place are connected to two micro-switches each. These micro-switches are tripped if the screw is even partially removed. One screw with its corresponding pair of micro-switches is used for tamper detection while power is off, and the other is used for tamper detection while power is on. Both screws must be removed in order to remove the cover of the module. Any unauthorized attempts to remove the cover results in the automatic tamper response, which occurs whether the appliance is powered on or not.

Any attempt to restart the appliance automatically displays tamper alerts on the Console.

Only a Reset Tamper operation performed by the appliance administrator can set the DocuSign Signature Appliance back to an operational state.

During the Reset Tamper Operation, the appliance administrator is required to plug-in the Backup MiniKey (described in [Chapter 3: Installing DocuSign Signature Appliance](#)).

In addition, external Tamper Evident cans provide physical evidence of any attempt to tamper with the module cover. The Tamper Evident cans are placed over the screws that join the top cover and bottom enclosure. The Tamper Evident cans are installed at the manufacturing stage.

The DocuSign Signature Appliance should be **constantly monitored** to make sure the device is not tampered with and that there is no unauthorized access to the appliance.

Recommended OTP Devices

It is recommended to select OTP devices that have the following characteristics:

- The OTP device has mechanisms that deny access to the security sensitive information of the OTP device. These may be tamper evident or tamper response mechanisms that provide evidence to the user that his/her device was tampered with, or more active mechanisms that disable the device if tampering occurs.
- The OTP device cannot be duplicated. This prevents the possibility of a hostile user signing on behalf of the legitimate user who holds the original OTP device.
- Each OTP device has a unique identification. This is necessary to enable binding a different OTP device to every user.

The OTP devices should be distributed in a secure manner to the end users, if applicable.

Using SAML Tickets to Authenticate Users

You can log into DocuSign Signature Appliance using a SAML ticket.

When a user presents a SAML token for the first time, an account is created for the user and the user can start signing. At any subsequent session, the user is required to present a new valid SAML ticket.

One of the benefits of accepting SAML tickets for authenticating users is to make DocuSign Signature Appliance services available to new user communities. For example, suppose Company A would like to enable users from company B to connect to DocuSign Signature Appliance services offered by Company A. Using SAML tickets, Company A does not have to register each of the requesting users. The fact that the users were provided with SAML tickets indicates they are trusted by Company B.

A popular product that enables issuing SAML tickets in Active Directory is Microsoft ADFS.

For more information, refer to [ADFS Flow](#) and to Microsoft documentation, such as: <http://msdn.microsoft.com/en-us/library/bb897402.aspx>.

Note: SAML tickets can be used only if DocuSign Signature Appliance is installed in Directory Independent mode.
SAML tickets cannot be used if DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode.

ADFS Flow

The ADFS/SAML workflow is as follows:

1. The end user authenticates to the local Active Directory based on the configuration of the local Active Directory deployment. For example, a Kerberos-based authentication may be used.
2. Following successful authentication, the local active directory provides the end user with a SAML ticket. This SAML ticket is a proof of authentication by the local ADFS, which is signed with the local ADFS key.
3. As part of the communication of the local user with the remote DocuSign Signature Appliance, the SAML ticket is presented to the remote DocuSign Signature Appliance service, and the DocuSign Signature Appliance validates the signature of the local ADFS system.
4. After the SAML ticket is approved for the first time, an account is created for the user and the user can start signing. At any subsequent session, the user is required to present a new valid SAML ticket.

Note: The SAML ticket is signed using the ADFS signing key accompanied by a certificate. The certificate should be given by a WorldWide Verifiable (WWV) Certificate Authority, so that the DocuSign Signature Appliance can validate the certificate of the SAML ticket.

Note: It is also possible to use a SAML ticket that is based on a non-WWV certificate, but in this case the entire certificate chain must be trusted by DocuSign Signature Appliance and should be loaded to DocuSign Signature Appliance using the **All Tasks → Subordinate CA → Load ROOT Cert Chain** option in the Control Panel.

Passive Mode using the Web App and Connector for SharePoint

If an organization would like to enable users from another organization to sign via a web application, the organization can deploy Web App in the same IT environment as the deployed DocuSign Signature Appliance. When a web application is used, the SAML based authentication process proceeds as follows:

1. The end user connects to his organizational URL in the Web App that is dedicated to that user's organization.
2. The Web App redirects the user to the user's local ADFS provider. During this process, the user is authenticated by his/her local Active Directory and receives a SAML ticket.
3. The user is redirected back to the Web App with the provided SAML ticket.
4. The Web App accesses the DocuSign Signature Appliance with the supplied SAML ticket. If this is a first time user, a new account is generated for this user. If the user already has an account, the account will be used.
The user is identified by his email address, which is part of the SAML ticket. It is assumed that the email address is unique.
5. The user continues with his/her web session.

Note: If the Connector for Microsoft SharePoint is deployed, the redirection of the user to the local ADFS provider is handled by Microsoft SharePoint. Further information is provided in the Connector for SharePoint User Guide

This mode is called Passive mode because the end user's flow is automatic and does not require any installation or configuration on the part of the end user. This flow is therefore suitable for many clientless platforms such as tablets, smartphones, etc.

Active Mode Using the DocuSign Signature Appliance Client

If an organization would like to enable users from another organization to sign via a desktop application, the end users must install the DocuSign Signature Appliance client and configure the DocuSign Signature Appliance client to use SAML based authentication. For more information, refer to the *DocuSign Signature Appliance Client User Guide*.

SAML Ticket Requirements

The SAML tickets must meet the following requirements to receive approval by the DocuSign Signature Appliance:

- The SAML ticket must be version 1.1 or version 2.0.
- Date/Time restriction – Every SAML ticket is valid for a given period. Make sure to provide SAML tickets that are still valid.
- The SAML ticket may include the following parameters:
 - **upn** – The user's identity. Mandatory
 - **emailaddress** – The user's email address. Mandatory
 - **Common Name** – the common name of the user. Mandatory
 - **Group** – The group name of the user, which is the user's organizational ID. This parameter is mandatory if the *SAML Working Method* system parameter has a value of 2.
 - **Audience** – This mandatory field should contain a URL that defines the DocuSign Signature Appliance Service. This URL should be identical to the URL defined in the DocuSign Signature Appliance *Accepting Relying Parties Tickets* system parameter.
 - Additional fields such as **name** and **surname**. These fields are optional.
- The SAML ticket must include a standard XML digital signature generated by the local ADFS server. The local ADFS server must be certified by a trusted worldwide verifiable CA. If groups are mandatory, the certificate thumbprint is validated against the thumbprint of the certificate that exists in the group record.

Note: Many of the SAML ticket parameters names (such as **upn** or **emailaddress**) can be modified in the [SAML](#) section of the DocuSign Signature Appliance system parameters.

Chapter 3: Installing DocuSign Signature Appliance

The following chapters describe how to install and uninstall DocuSign Signature Appliance, manage the DocuSign Signature Appliance system, and connect to and use the DocuSign Signature Appliance console.

DocuSign Signature Appliance installation consists of several steps:

1. Installing the administrative client. The administrative client includes various administrative utilities, as well as the Microsoft Management Console (MMC), the administration snap-in. The administrative client installation is described in this chapter.
2. Installing the Central Enterprise/Central FIPS appliance hardware. Appliance hardware installation is described in this chapter.
3. Installing the DocuSign Signature Appliance software, in either a Microsoft-Active Directory, LDAP based directory, or Directory Independent environment (including installing DocuSign Signature Appliance in Common Criteria EAL4+ mode). Appliance software installation is described in this chapter.
4. Deploying the DocuSign Signature Appliance Client, in a Microsoft-Active Directory environment, LDAP based directory, or Directory Independent environment. This is described in [Chapter 4: Deploying the DocuSign Signature Appliance Client](#).
5. Using the DocuSign Signature Appliance console. This is described in [Chapter 6: Using the Consoles](#).
6. Using the graphical signature management application that enables setting a graphical signature for users of the organization. This is described in [Using the Graphical Signature Management Application](#).
7. Optionally setting up the organization in a high availability configuration, in which several DocuSign Signature Appliances are set up to provide load balancing and redundancy. This is described in [Chapter 7: Configuring High Availability](#).

Note: Installation differs slightly depending on whether DocuSign Signature Appliance is being installed in a Microsoft Active Directory environment, LDAP based environment, or Directory Independent environment. These differences are mentioned where applicable.

Installing the Administrative Client

The administrative client includes various administrative utilities. The administrative client enables you to administrate the following components:

- Administrate appliances, using the Administration MMC. For more information, refer to [Chapter 5: Managing the DocuSign Signature Appliance](#)
- Administrate users. For more information, refer to [Using the Users Management Utility](#).
- Set end users configuration. For more information, refer to [Chapter 8: Configuration Utility](#).
- Set graphical signatures for users. For more information, refer to [Using the Graphical Signature Management Application](#).

Installation Requirements

The administrative client requires the administrative station to have one of the following operating systems:

- Windows 2008/Windows 2008 R2.
- Windows 7
- Windows 8
- Windows 10
- Windows 2012 Server.

Note: The DocuSign Signature Appliance client can be also be installed in any 64 bit variant of the above operating systems, such as Windows 7 64 bit.

When installing the administrative client in a Microsoft Active Directory environment, the administrative station must be joined to the Microsoft Domain. In addition, the administrator who is installing the administrative client must have domain administrative rights.

Note: It is possible for a user with limited permissions to install DocuSign Signature Appliance in an Active Directory environment. This situation is relevant for organizations where DocuSign Signature Appliance serves only certain organizational units. This type of installation requires performing certain preparations prior to installing DocuSign Signature Appliance, as well as performing certain actions after DocuSign Signature Appliance was installed. Refer to [Appendix A: Installation with Reduced Privileges](#) for detailed information on how to install DocuSign Signature Appliance using a user with limited permissions.

Note: The administrative client software installs the administrative client along with other administrative components, such as the graphical signature management capabilities and administrative utilities.

Installing the Administrative Client

Note: You must install the administrative client on your administrative station before installing the DocuSign Signature Appliance.

To install the administrative client:

- Insert the ARX CoSign CD into the CD drive. The *ARX CoSign Client Installation* screen appears:



Figure 2 ARX CoSign Client Installation Screen

- Select the following components:
 - **ARX CoSign Client.**
 - **ARX CoSign Admin.**
- Click **Install Now.**

When installation is complete, a success message appears.

Uninstalling the Administrative Client

To uninstall the administrative client, uninstall all components, as follows:

1. Open the **Start** menu and select **Programs → ARX CoSign → Uninstall CoSign Components.**
2. A confirmation box appears. Click **Yes** to uninstall. The uninstalling process begins.
3. When the client is uninstalled from the workstation, a message box appears to inform you that the system finished uninstalling. Click **OK.**

The administrative client is uninstalled from the workstation.

Installing the DocuSign Signature Appliance Hardware version 8.0

The following sections provide instructions for installing the DocuSign Signature Appliance hardware version 8.0 models:

- DocuSign Signature Appliance Central FIPS Appliance Hardware version 8.0 – refer to [Installing the DocuSign Signature Appliance Central FIPS Appliance Hardware 8.0](#)
- DocuSign Signature Appliance Central Enterprise Appliance Hardware version 8.0 – refer to [Installing the CoSign Central Enterprise Appliance Hardware v7.0 and 8.0.](#)

Installing the DocuSign Signature Appliance Central FIPS Appliance Hardware 8.0

The DocuSign Signature Appliance Central FIPS appliance hardware (shown in Figures 3 and 4) includes:

- A vent for the inner fan.
- Three LEDs – Power, Hard Disk, and Tamper.
- A USB connector for inserting MiniKey tokens.
- A power switch
- A touch screen for basic console information.
- Dual power supply.
- Two Ethernet connectors for connecting to the network. One for the regular secure interface and one dedicated for the Web Console (IP address 10.0.0.2).



Figure 3 DocuSign Signature Appliance Central FIPS v8.0 Front Panel



Figure 4 DocuSign Signature Appliance Central FIPS v.8.0 Back Panel

The following table lists the physical dimensions of the DocuSign Signature Appliance Central FIPS v8.0 appliance.

Width	42.5 cm (16.7")
Length (Depth)	48.2 cm (18.9")
Height	13 cm (5.1")
Weight	13.5 kg (30 lb)

To install the DocuSign Signature Appliance Central FIPS v8.0 appliance hardware:

1. Verify that you have all the necessary sets of keys and MiniKey (USB) tokens, as follows:
 - Two backup MiniKey tokens. Each of the backup MiniKey tokens contains identical secrets, which include several triple DES Keys that are generated during the installation of the DocuSign Signature Appliance software. These keys are used for encrypting the backup file and the private keys in the database.

The keys also serve a role in database replication, which is an integral component of a High Availability configuration (refer to [Chapter 7: Configuring High Availability](#)).

Note: The backup MiniKey token that was supplied with CoSign versions prior to version 5, is not compatible with Appliance version 8.0. Please contact DocuSign for information on how to duplicate the backup tokens so that they are compatible with DocuSign Signature Appliance version 8.0.

- One license MiniKey token. The license MiniKey token must be inserted while operating the DocuSign Signature Appliance. If the license MiniKey token is not inserted, the appliance automatically shuts down after two hours. In this case, the Event Log and the console display messages indicating that the license MiniKey token is not inserted.

Note: The license MiniKey limits the number of end-users that may use the DocuSign Signature Appliance. If you require additional user licenses, please contact your ARX sales representative.

Note: Starting from CoSign version 7.5, the license Minikey token may have an expiration date.
Refer to [Displaying Status](#) for instructions on how to view the expiration date.
Refer to [Obtaining a New License](#) for instructions on how to obtain an updated license.

- A physical key for front panel locking.
2. The DocuSign Signature Appliance Central FIPS box is rack mountable. Install DocuSign Signature Appliance Central FIPS in the rack as follows:
 - Insert a rack shelf in the rack.
Follow the instructions in the rack's guide to properly attach the shelf to the rack.
 - Carefully place the DocuSign Signature Appliance Central FIPS box on the shelf.
 - Use a screw driver, 4 screws, 4 washers, and 4 nuts to secure the DocuSign Signature Appliance Central FIPS box to the front vertical rail of the rack.
Use the four holes in the front of the DocuSign Signature Appliance Central FIPS box.

Caution: Make sure that the rack has no overload limitations that exceeds the weight of the appliance as defined in the above *physical dimensions* table.

3. Connect the appliance to the dual power supply.
4. Connect the appliance to the network using the Main Ethernet connector and a standard Ethernet cable. DocuSign Signature Appliance supports 10/100/1000 Mb/s Ethernet connections. You can also connect, as needed, the Web Console platform to the DocuSign Signature Appliance via the dedicated administrative network interface.

Caution: Use shielded network cables.

5. On the DHCP server, you can set up a specific IP address for the DocuSign Signature Appliance appliance based on the appliance's MAC address. The appliance's MAC address is located on the back panel of the appliance (refer to Figure 6).

Note: To use a static IP address, you must set the appliance's network parameters using the console. For more information on using the console, refer to [Chapter 6: Using the Consoles](#).

6. On the back panel of the appliance, connect the dual power supply to the power networks.
7. On the front panel of the appliance, press the power switch.

Caution: There is a risk of explosion if the battery is replaced with an incorrect type of battery. Dispose of used batteries according to the manufacturer's instructions.

Environmental Conditions

The following table lists the environmental conditions:

	Operating	Non-operating
Ambient Temperature	41 to 104°F 5 to 40°C	- 4 to 149°F - 20 to 65°C
Relative Humidity	20 to 80 % (non-condensing)	10 to 90 % (non-condensing)

Caution: Make sure that the temperature inside the rack does not exceed the temperatures listed in the above *Environmental Conditions* table. Note that temperatures inside the rack can sometimes exceed the service room temperature.

Caution: When installing the appliance in a rack, make sure that the amount of air flow required for the safe operation of the equipment is not compromised.

Note: The Appliance is permitted for connection to an IT power distribution system in Norway.

DocuSign Signature Appliance Central FIPS/Common Criteria Certificates

The DocuSign Signature Appliance Central FIPS appliance complies with the following certificates:

- UL file No: *pending* with the following conditions:
 - Indoor usage only.
 - The box has been judged on the basis of the required spacing in the Standard for Safety of Information Technology Equipment, including Electrical Business Equipment.
 - Electrical rating of power supply:
 - Rated Voltage: 100-127 Vac/200-240 Vac
 - Input Current: 5.8A/2.9A
 - Frequency: 50/60 Hz

Caution: Make sure that the electricity circuit is not overloaded by the electrical consumption of the appliance as defined in the above list.

This may entail taking overcurrent protection and supply wiring measures.

Caution: Make sure that the rack has reliable earthing. Particular attention should be given to supply connections other than direct connection to the branch circuit (e.g., use of power strips).

- The following warning is presented: “DANGER! Incorrect replacement of battery can cause explosion. Replace only with the same or equivalent type of battery recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions”.
- FIPS 140-2 level 3 validation:
 - Certificates number *pending*.
- Common Criteria EAL4+ validation:
 - Certificates number *pending*.

Warning: Before performing hardware maintenance based service, remember to disconnect the appliance from the two power sources.

Installing the CoSign Appliance Hardware version 7.0

The following sections provide instructions for installing the various CoSign appliance models.

- [Installing the CoSign Central FIPS Appliance Hardware](#) version 7.0.
- [Installing the CoSign Central Enterprise Appliance Hardware](#) v7.0 and 8.0.

Installing the CoSign Central FIPS Appliance Hardware version 7.0

The CoSign Central FIPS appliance hardware (shown in Figures 5 and 6) includes:

- A vent for the inner fan.
- A protective metal door with a lock.
- Three LEDs – Power, Hard Disk, and Tamper.
- A USB connector for inserting MiniKey tokens.
- Two power switches (one on the front panel of the appliance and one in the back of the appliance).
- A built-in console, consisting of a display and 4-button keypad.
- A power connector.
- An Ethernet connector for connecting to the network.

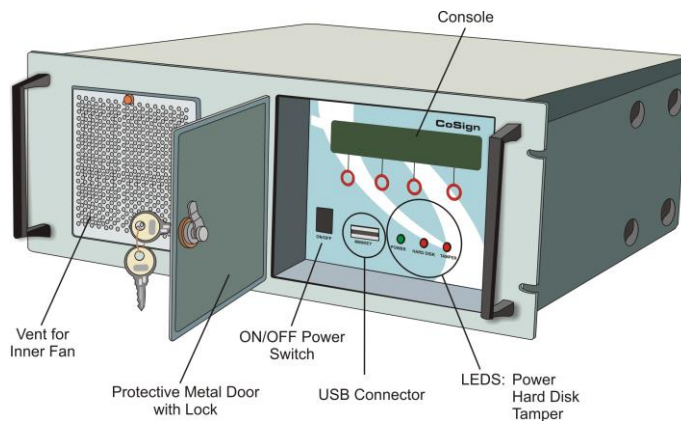


Figure 5 CoSign Central FIPS v7.0 Front Panel

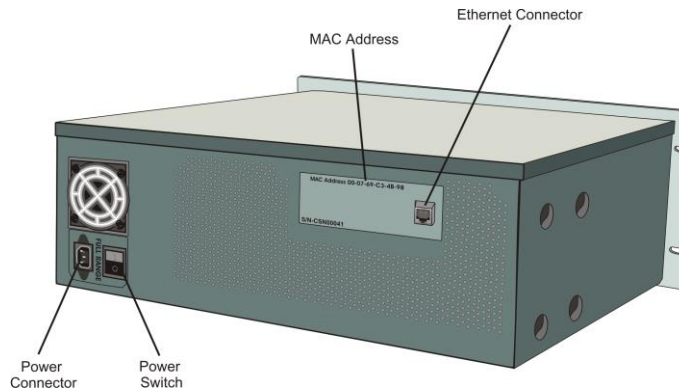


Figure 6 CoSign Central FIPS v7.0 Back Panel

The following table lists the physical dimensions of the CoSign Central FIPS v7.0 appliance.

Width	48.3 cm (19")
Length (Depth)	44.7 cm (17.6")
Height	17.8 cm (7")
Weight	15 kg (33 lb)

To install the CoSign Central FIPS appliance hardware:

- Verify that you have all the necessary sets of keys and MiniKey (USB) tokens, as follows:
 - Two backup MiniKey tokens. Each of the backup MiniKey tokens contains identical secrets, which include several triple DES Keys that are generated during the installation of the CoSign appliance software. These keys are used for encrypting the backup file and the private keys in the database.
The keys also serve a role in database replication, which is an integral component of a High Availability configuration (refer to [Chapter 7: Configuring High Availability](#)).
 - One license MiniKey token. The license MiniKey token must be inserted while operating the CoSign appliance. If the license MiniKey token is not inserted, the appliance automatically shuts down after two hours. In this case, the Event Log and the console display messages indicating that the license MiniKey token is not inserted.

Note: The license MiniKey limits the number of end-users that may use the CoSign appliance. If you require additional user licenses, please contact your ARX sales representative.

Note: Starting from CoSign version 7.5, the license Minikey token may have an expiration date.

Refer to [Displaying Status](#) for instructions on how to view the expiration date.

Refer to [Obtaining a New License](#) for instructions on how to obtain an updated license.

- A physical key for front panel locking.
- The CoSign Central FIPS box is rack mountable. Install CoSign Central FIPS in the rack as follows:

- Insert a rack shelf in the rack.
Follow the instructions in the rack's guide to properly attach the shelf to the rack.
 - Carefully place the CoSign Central FIPS box on the shelf.
 - Use a screw driver, 4 screws, 4 washers, and 4 nuts to secure the CoSign Central FIPS box to the front vertical rail of the rack.
Use the four holes in the front of the CoSign Central FIPS box.
3. Connect the appliance to the power supply.
 4. Connect the appliance to the network using the Ethernet connector and a standard Ethernet cable. CoSign supports 10/100/1000 Mbits/sec Ethernet connections.

Caution: Use shielded network cables.

5. On the DHCP server, you can set up a specific IP address for the CoSign appliance based on the appliance's MAC address. The appliance's MAC address is located on the back panel of the appliance (refer to Figure 6).

Note: To use a static IP address, you must set the appliance's network parameters using the console. For more information on using the console, refer to [Chapter 6: Using the Consoles](#).

6. On the back panel of the appliance, turn on the power switch.
7. On the front panel of the appliance, press the ON/OFF power switch.

Caution: There is a risk of explosion if the battery is replaced with an incorrect type of battery. Dispose of used batteries according to the manufacturer's instructions.

Environmental Conditions

The following table lists the environmental conditions:

	Operating	Non-operating
Ambient Temperature	41 to 95°F 5 to 35°C	- 4 to 149°F - 20 to 65°C
Relative Humidity	20 to 80 % (non-condensing)	10 to 90 % (non-condensing)

Caution: Make sure that the temperature inside the rack does not exceed 35°C / 95°F.

CoSign Central FIPS and Common Criteria Certificates

The CoSign Central FIPS appliance complies with the following certificates:

- UL file No: E192352, with the following conditions:
 - Indoor usage only.
 - The box has been judged on the basis of the required spacing in the Standard for Safety of Information Technology Equipment, including Electrical Business Equipment.

- Electrical rating of power supply:
- Voltage: 100-240 Vac
- Frequency: 60/50 Hz
- Current: 10 A
- The following warning is presented: “DANGER! Incorrect replacement of battery can cause explosion. Replace only with the same or equivalent type of battery recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions”.
- FIPS 140-2 level 3 validation:
 - Certificates number 887, 1208, 1422.
- Common Criteria EAL4+ certification:
 - For CoSign version 7.1 and version 7.5

Installing the CoSign Central Enterprise Appliance Hardware v7.0 and 8.0

Note: The following installation instructions apply both to hardware version 7.0 and hardware version 8.0 of the CoSign Central Enterprise Appliance.

The CoSign Central Enterprise appliance hardware (shown in Figures 7 and 8) includes:

- Power supply and cable.
- A recessed power button on the front panel.
- An Ethernet connector for connecting to the network in the back panel.
- A serial connector for connecting a terminal in the back panel.
- Front panel USB connectors for inserting MiniKey tokens.

Note: Do not connect any of the other interfaces.



Figure 7 CoSign Central Enterprise Front Panel



Figure 8 CoSign Central Enterprise Back Panel

The following table lists the dimensions of the CoSign Central Enterprise appliance version 7.0.

Width	47.9 cm (18.8")
Length (Depth)	55.88 cm (22")
Height	4.45 cm (1.75")
Weight	12.7 kg (25.4 lbs)

The following table lists the dimensions of the DocuSign Signature Appliance Central Enterprise appliance version 8.0 (M3).

Width	44 cm (17.3")
Length (Depth)	55.9 cm (22")
Height	4.3 cm (1.7")
Weight	12.7 kg (28 lbs)

The following table lists the dimensions of the DocuSign Signature Appliance Central Enterprise appliance version 8 (M5).

Width	43.5 cm (17.1")
Length (Depth)	57.6 cm (22.7")
Height	4.3 cm (1.7")
Weight	12.3 kg (27.1 lbs)

To install the DocuSign Signature Appliance Central Enterprise appliance hardware:

1. Verify that you have all the necessary sets of keys and MiniKey (USB) tokens, as follows:
 - Two backup MiniKey tokens. Each of the backup MiniKey tokens contains identical secrets, which include several triple DES keys that are generated during the installation of the

DocuSign Signature Appliance Enterprise appliance software. These keys are used for encrypting the backup file and the private keys in the database.

- License MiniKey token. The license MiniKey token must be inserted while operating the DocuSign Signature Appliance Central Enterprise appliance. If the license MiniKey token is not inserted, the appliance automatically shuts down after two hours. In this case, the Event log displays messages indicating that the license MiniKey token is not inserted.

Note: The license MiniKey limits the number of end-users that may use the DocuSign Signature Appliance Central Enterprise appliance. If you require additional user licenses, contact your ARX sales representative.

2. Connect the power cable to the DocuSign Signature Appliance Central Enterprise's power connector, and then connect the power cable to the power supply.
3. Connect the appliance to the network using the Ethernet connector and a standard Ethernet cable. DocuSign Signature Appliance Central Enterprise supports 10/100/1000 Mb/s Ethernet connections.

Caution: Use shielded network cables.

4. On the DHCP server, you can set up a specific IP address for the DocuSign Signature Appliance Central Enterprise appliance based on the appliance's MAC address. The appliance's MAC address is located on the back panel of the appliance.

Note: To use a static IP address, first connect the console terminal to the serial connector of the DocuSign Signature Appliance Central Enterprise appliance. For more information on using the console, refer to [Chapter 6: Using the Consoles](#).

5. On the front panel of the appliance, press the recessed power button.

Environmental Conditions

The following table lists the environmental conditions:

	Operating	Non-operating
Ambient Temperature	50 to 95°F 10 to 35°C	-40 to 140°F -40 to 60°C
Relative Humidity	8 to 80 % (non-condensing)	8 to 80 % (non-condensing)

Caution: Make sure that the temperature inside the rack does not exceed 35°C / 95°F.

Installing the Appliance Software

The Appliance Software can be installed in either a Microsoft Active Directory environment, LDAP environment, Directory Independent Environment or in a Common Criteria EAL4+ Environment.

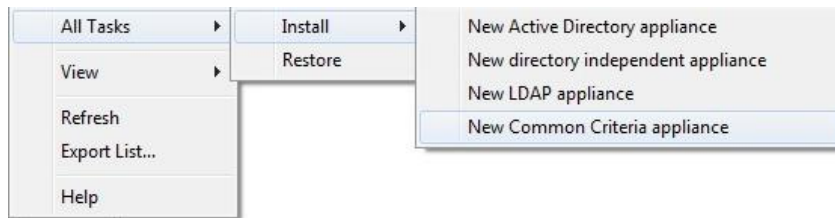


Figure 9 Installation Options

Note: The following software installation instructions apply for all DocuSign Signature Appliance Central hardware models, unless otherwise noted.

Note: In the future DocuSign Signature Appliance version 8.2, an additional entry for installing a *New Common Criteria Seal appliance* option will appear for installing DocuSign Signature Appliance as a Seal Creation Device.

Installing DocuSign Signature Appliance in a Microsoft Active Directory Environment

The DocuSign Signature Appliance interface to Microsoft Active Directory assists both administrators and end users in the following aspects:

- *Administrators* – The administrator does not need to manage users in DocuSign Signature Appliance since it can be instructed to automatically synchronize with the users located in the Microsoft Active Directory. Depending on DocuSign Signature Appliance’s configuration, each time a new user is created in the Active Directory, the DocuSign Signature Appliance generates a new user account. Additionally, depending on the DocuSign Signature Appliance Internal certificate authority configuration, a private key and a certificate are generated for the user. When certain attributes in the user record in the directory are modified (such as the user's email address), a new certificate is generated for the user by the DocuSign Signature Appliance. When the user is deleted from the directory, the user is also deleted from the DocuSign Signature Appliance and his/her certificate is revoked.

In addition, the DocuSign Signature Appliance also publishes information in the domain, enabling the user to easily access it automatically. For example, the availability status of the DocuSign Signature Appliance or the Root CA certificate is published at the Microsoft Active Directory as well.

- *Users* – When using active directory, DocuSign Signature Appliance can employ the Kerberos ticketing mechanism to enable users to automatically logon to the DocuSign Signature Appliance using the credentials supplied at the beginning of the user's session in the Microsoft Domain. In this case, it is mandatory that the user's machine be joined to the Microsoft domain.

You can install DocuSign Signature Appliance in a multiple trusted Active Directory (AD) environment, where a single DocuSign Signature Appliance installed in a certain AD Domain can accept users from other domains that have mutual trust with DocuSign Signature Appliance's domain.

In this mode of work, users' synchronization works differently: upon first access of a new user, DocuSign Signature Appliance automatically creates an account for the user and, depending on the configuration, also generates a key and a certificate for the user.

Upon an update of the user information in the domain, an updated certificate is generated for the user, depending on the updated parameters.

When the user is deleted from the domain, the user account is deleted from DocuSign Signature Appliance, and his/her certificate is revoked.

In order to manage DocuSign Signature Appliance after installation, you must be either a member of the administrators group and be a valid DocuSign Signature Appliance user (as defined in the *Directory Setup* dialog box, shown in Figure 14), or be the built-in DocuSign Signature Appliance administrator.

Permission Considerations

Since the installation of the DocuSign Signature Appliance requires access to Microsoft Active Directory in several locations in the Directory, special care must be taken in using the appropriate administrator accounts. Regarding the permissions of the administrator installing DocuSign Signature Appliance in a Microsoft Active Directory environment, there are three approaches:

- *Straightforward installation by an administrator with full permissions.* The DocuSign Signature Appliance software is installed from the Appliances Management application. In this installation scenario, the administrator logged on to the administration workstation that is running the DocuSign Signature Appliance administrative client is a member of both the Enterprise admins and Domain admins groups. This is because one of the operations that are performed during the installation is the creation of a new computer entry in the Microsoft Active Directory.
- *Installation by an administrator with limited permissions.* This situation is relevant to organizations where DocuSign Signature Appliance serves only certain organizational units. This type of installation requires performing certain preparations prior to installing DocuSign Signature Appliance, as well as performing certain actions after DocuSign Signature Appliance was installed.
Refer to [Appendix A: Installation with Reduced Privileges](#) for detailed information on how to install DocuSign Signature Appliance using a user with limited permissions.
- *Installation by an administrator who may not have full permissions.* If the administrator does not have permissions for all Active Directory related activities that occur during the installation, a window appears, detailing the exact problem. The exact returned error is displayed in the bottom of the window.



Figure 10 Switching to a Different Administrator

You can switch to another administrator account that may have the permissions to perform the failed operation. You can also specify whether to continue using the new administrator account for the next operations.

For example, if DocuSign Signature Appliance is installed in a child domain environment, the installation can start with an administrator of the child domain using a workstation that is joined to the child domain. During the installation, it is required to also access the parent domain for updating the parent domain with information such as the CA certificate and the CA CRL. If the administrator of the child domain does not have parent domain permissions, the window shown in Figure 10 appears, requesting the user to supply an administrator account with administrative permissions in the parent domain.

Installation Instructions

To install the DocuSign Signature Appliance software:

1. Activate the Control Panel by opening the **Start** menu and selecting **Programs** → **ARX CoSign** → **CoSign Control Panel**. The CoSign Control Panel appears.
2. Select **Appliances Management**. The *ARX CoSign Appliance Management* window appears.
3. Right-click **CoSign appliances** and select **All Tasks** → **Install** → **New Active Directory appliance**. The License Agreement appears.
4. Accept the license agreement and click **Next**. The *Network Setup* dialog box appears.

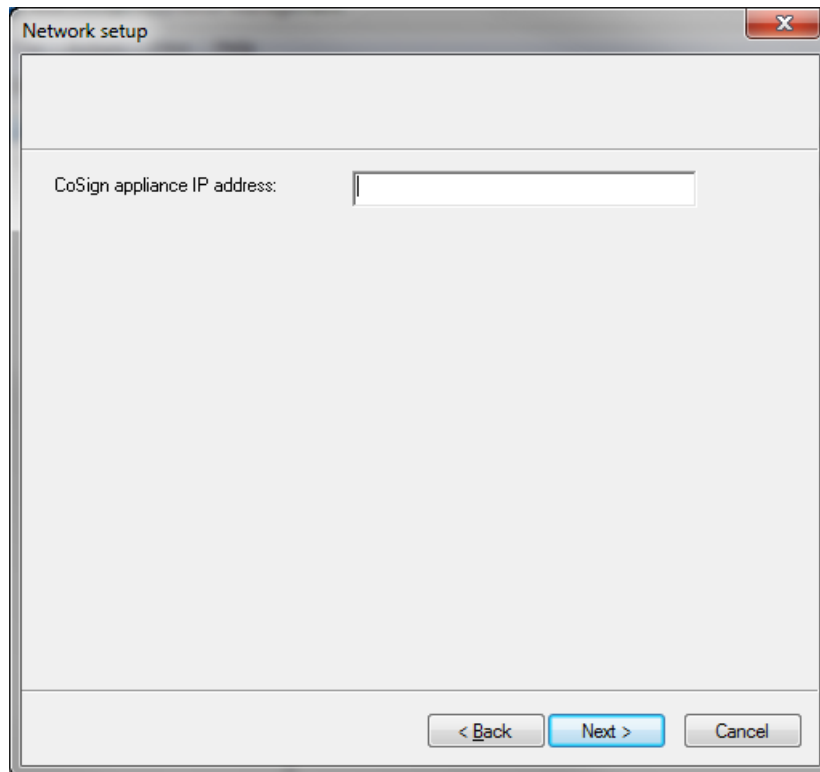


Figure 11 Network Setup Dialog Box

- Enter the IP address of the DocuSign Signature Appliance. This parameter is necessary for enabling basic communication to and from the DocuSign Signature Appliance. Starting from DocuSign Signature Appliance hardware version 8.0, IPv6 is also supported. You can enter an IPv6-type IP address in the **CoSign appliance IP address** field.

Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to [Using a Static IP Address](#) and [Enabling DHCP](#).

Note: Make sure that your DHCP server is set up to allocate the correct DNS server address for the domain. If it is not set up, use the console to set a DNS server address before installing DocuSign Signature Appliance (refer to [Using a Static IP Address](#)).

- Click **Next**. The *CoSign Administrator User* dialog box appears.

CoSign administrator user

Enter a user name and a password of a built-in administrator who will manage the CoSign appliance. Do not forget this password, since without remember the password you will not be able to perform important administrative tasks

Admin user name:

Admin password:

Confirm admin password:

< Back Next > Cancel

Figure 12 CoSign Administrator User Dialog Box

- Enter the user name and password of a built-in administrator who will manage the DocuSign Signature Appliance. You will need to enter the password again for confirmation. The built-in administrator is very useful in cases where the Active Directory-based administrator has a problem connecting to DocuSign Signature Appliance.

Note: Make sure to select an appropriate password for this user since the administrator user name and password that you enter in this dialog box are used for appliance management. During installation, a new user is generated in DocuSign Signature Appliance with this user name and password.

Make sure not to forget this password, since without it you will not be able to perform any administrative task.

8. Click **Next**. The *Active Directory Admin Account* dialog box appears.

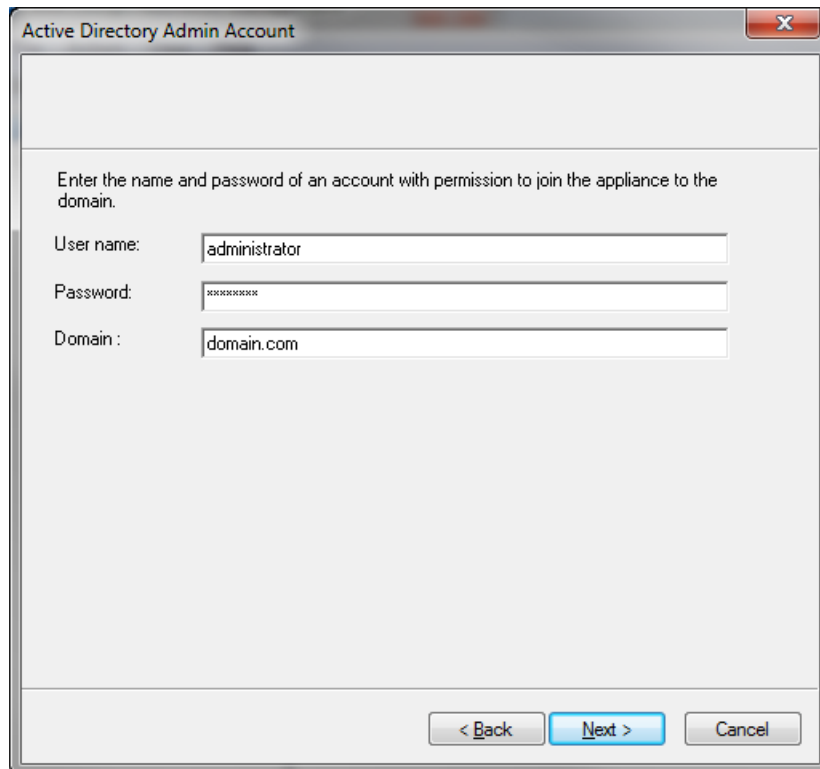
The image shows a Windows-style dialog box titled "Active Directory Admin Account". It contains a text area with the instruction: "Enter the name and password of an account with permission to join the appliance to the domain." Below this are three input fields: "User name:" with the value "administrator", "Password:" with a masked password "xxxxxxxx", and "Domain:" with the value "domain.com". At the bottom of the dialog are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

Figure 13 Active Directory Admin Account Dialog Box

Note: The *Active Directory Admin Account* dialog box includes default values based on the administrative user who is currently logged on. You can change the default values if desired. If default values do not appear, the DNS configuration of the administration station may be problematic and the installation procedure may fail (refer to [Default Values Do Not Appear in the Directory Setup Dialog Box](#)).

- Enter an administrative account that has permission to join the DocuSign Signature Appliance to the Domain.
- Click **Next**. The *Directory Setup* dialog box appears.

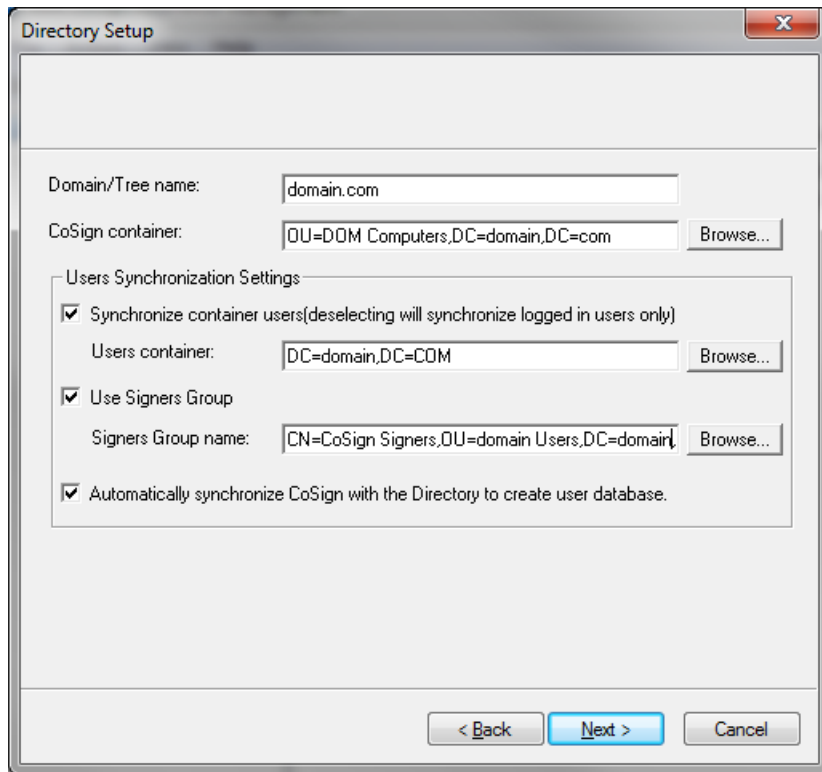


Figure 14 Directory Setup Dialog Box

Note: The *Directory Setup* dialog box includes default values based on the administrative user who is currently logged on. You can change the default values if desired. If default values do not appear, the DNS configuration of the administration station may be problematic and the installation procedure may fail (refer to [Default Values Do Not Appear in the Directory Setup Dialog Box](#)).

Note: If DocuSign Signature Appliance is intended to be installed in a regional domain of a forest, set the above fields to include information of the regional domain and **not** of the ROOT domain.

- Enter the following information:
 - **Domain/Tree name** – The name of the domain that contains the DocuSign Signature Appliance.
 - **CoSign container** – The location in the Active Directory where the DocuSign Signature Appliance computer will be contained. A new computer entry will be created in this location. You can click **Browse** to browse to the appropriate location. The *Directory Object Selection Tree* dialog box appears.

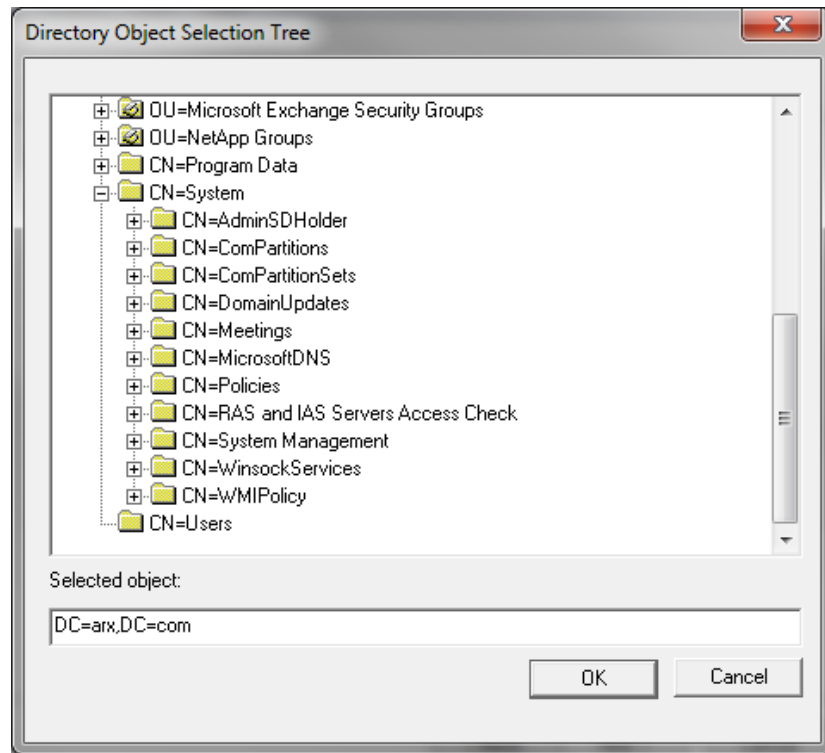


Figure 15 Directory Object Selection Tree Dialog Box

Note: If the Administration MMC is being used on the domain machine, the displayed default values will be different than those for a regular machine. Modify these values as required.

- **Users Synchronization Settings** – If you do not select this option, the DocuSign Signature Appliance will work in a multiple Active Directory environment. This means that users from several domains that have trust between the domains can use DocuSign Signature Appliance to perform signature operations. The user must belong to the specified signers group. The first attempt of the user to access the DocuSign Signature Appliance will automatically generate an account for the user and, depending on the system configuration, will also generate a key and a certificate for the user.

If you do select this option, then using the values you enter in the *Directory Setup* dialog box (Figure 14), the DocuSign Signature Appliance selects the users of the domain who will be considered DocuSign Signature Appliance users and thus will be able to sign documents. The selection is performed as follows: In the first stage, all users defined in the Users Container can be potential users of the DocuSign Signature Appliance.

In the next stage, if **Use Signers Group** is selected, only users who belong to the specified group are valid DocuSign Signature Appliance users. Note that in the Signers group it is possible to define additional subgroups to ease the selection of DocuSign Signature Appliance users. For example, the administrator can define that the Signers group include the Sales and Marketing groups.

- **Users container** – The general scope of users who can access DocuSign Signature Appliance, based on a sub-tree of users in the Active Directory. You can click **Browse** to browse to an existing location of the Users container in Active Directory. The *Directory Object Selection Tree* dialog box appears (Figure 15).

- **Use Signers Group** – Select this option to specify that only users who belong to the Signers group be defined as DocuSign Signature Appliance users.
- **Signers Group Name** – The full distinguish name of the Signers Group. Click **Browse** to browse to the location of the Signers Group. Remember to specify the name of the Signers Group in addition to the location of the group.
You can click **Browse** to browse to an existing location of the Signers Group in Active Directory. The *Directory Object Selection Tree* dialog box appears (Figure 15).
- **Automatically synchronize CoSign with the directory to create user database** – If this option is selected, DocuSign Signature Appliance will automatically generate accounts for each signer and, depending on the CA configuration, generate a key and a certificate for each signer. If this option is not selected, the administrator should perform a manual synchronization. This option should be used in cases where it is required to change settings after installation, but before user accounts are created.

Note: In addition to the default DocuSign Signature Appliance administrator, you can define additional DocuSign Signature Appliance administrators who are valid Active Directory users. If you do so, the DocuSign Signature Appliance administrator must also be located in this subtree and the Signers Group in order to be a valid DocuSign Signature Appliance user. Otherwise the administrator will not be able to administrate DocuSign Signature Appliance.

Important: *In the case of a regular AD installation*, do not modify the name of the sub-tree of DocuSign Signature Appliance users in the Active Directory. Such a modification can lead to deleting all the users and their information inside the DocuSign Signature Appliance.

Note: If you move a user from the DocuSign Signature Appliance OU (DocuSign Signature Appliance container) to a different location, the user is not automatically deleted from the DocuSign Signature Appliance. The next manual synchronization operation will delete the user from the DocuSign Signature Appliance. This means that the user's key, certificate, and graphical signature are deleted.

Note: If you move a user from the Signers group in the Active Directory, the user is not automatically deleted from the DocuSign Signature Appliance, but the users will be unable to connect to DocuSign Signature Appliance. The next manual synchronization operation will delete the user from the DocuSign Signature Appliance.

Note: In a multiple AD domain environment, user synchronization is based on two considerations:

- If the user is updated in the domain in a parameter that is relevant to DocuSign Signature Appliance (i.e., email address), the user will be updated in DocuSign Signature Appliance as well.
- If the user is deleted from the domain, the user will be deleted from DocuSign Signature Appliance as well and his/her certificate will be revoked.

- Click **Next**.
If the requested Signers groups does not exist, you are queried whether the installation procedure should create this group inside Active Directory.
After clicking **Yes** or **No**, the *CA Setup* dialog box appears.

Note: If a Signers group is created, valid DocuSign Signature Appliance users are created only after assigning users to the Signers group.

- Figure 16 CA Setup Dialog Box
- If you want the DocuSign Signature Appliance to use an internal Certificate Authority (CA) for generating end-user certificates, refer to [Installing an Internal Certificate Authority](#) for detailed explanations of the *CA Setup* dialog box. After setting up the internal CA in the *CA Setup* dialog box, continue with Step [4](#).
- If you want the DocuSign Signature Appliance to use a World Wide Verifiable Certification Authority (CA) for automatically generating end-user certificates, refer to [Using an External World Wide Verifiable CA in Automated Mode](#) for detailed explanations of the *CA Setup* dialog box. After configuring the World Wide verifiable CA in the *CA Setup* dialog box, continue with Step [4](#).
- If you do not wish the DocuSign Signature Appliance to use an internal CA, select the **Without CA** option in the **CA type** drop-down box. In this case, you will be using DocuSign Signature Appliance in manual external CA mode. It is highly recommended to read the section [Using DocuSign Signature Appliance in Manual External CA Mode](#) before installing DocuSign Signature Appliance with this option.
- Click **Next**. The installation begins. A status bar displays the status of the installation operation. During the installation, status messages appear on both the console display and the Administration MMC display.
 - At the **Please insert a backup Minikey** prompt, insert the first backup MiniKey token.
 - At the **Please insert a second backup Minikey** prompt, remove the first MiniKey token and insert the second backup MiniKey token. The second backup MiniKey is a duplicate of the first backup MiniKey.

- At the **Please insert your License Minikey** prompt, insert the license MiniKey token.

If you selected the option **Install as Subordinate CA** in the CA Setup dialog box (refer to [Installing an Internal Certificate Authority](#)), several dialog boxes appear, necessitating various operations. For detailed instructions, refer to [Installing DocuSign Signature Appliance as a Subordinate CA](#).

In all other cases, your part in the installation is complete.

If you did not select **Automatically synchronize CoSign with the directory to create user database** in the Directory Setup dialog box (Figure 14), a message appears, reminding you to perform a manual synchronization.

If you did select that option, the installation will generate user accounts and automatically generate keys and certificates for all created users. A progress bar continues to display the progress of the operation. The time needed for creating the users, keys, and certificates depends on the number of users and the selected key length.

- Click **Finish**.

Note: If the first stage of installation was unsuccessful, the DocuSign Signature Appliance returns to its factory settings. This enables you to rerun the installation. In this case, the status bar displays that installation was unsuccessful and you can click the **Back** buttons to modify settings before rerunning the installation.

If the installation was unsuccessful and you are unable to rerun the installation, restore DocuSign Signature Appliance to factory settings and then try again. For more information about restoring factory settings, refer to [Restoring Factory Settings](#).

Note: Clicking **Cancel** does not stop the installation process, it only closes the progress bar on the administration machine (unless you specified a subordinate CA installation).

- In the Administration MMC window, right-click **CoSign appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You will need to login and then you can manage DocuSign Signature Appliance using the Administration MMC (refer to [Chapter 5: Managing the DocuSign Signature Appliance](#)).

Note: Keep the license MiniKey token plugged into the device at all times. Unplugging the license MiniKey for several hours may shut down the service.

Periodically check the number of appliance users. If the number of users is approaching the license limit, contact ARX for a replacement license MiniKey token

If you received a license with an expiration date, periodically check it using the console to verify it is not about to expire. Refer to [Displaying Status](#) for instructions on how to view the expiration date. Contact ARX for a replacement license MiniKey token before the current key expires.

Note: In a high availability environment, the licenses of all the DocuSign Signature Appliances in the high availability site should have an identical limitation on the number of appliance users.

Note: Store the backup MiniKey in a separate, secure place (for example, a safe). In case of disaster, you can use the backup MiniKey and the backup file of the DocuSign Signature Appliance's database to safely recover and restore DocuSign Signature Appliance data. For more information on how to backup and restore the DocuSign Signature Appliance's database, refer to [Backing up the DocuSign Signature Appliance Data](#).

If you lose the backup MiniKey, you will not be able to perform some critical functions, such as

restoring the DocuSign Signature Appliance (even if you have a backup file), adding an alternate appliance, and performing a reset tamper operation. Therefore, make sure that the backup MiniKey, as well as the second backup MiniKey, will be available when needed.

The following table provides a summary of the users involved in the installation procedure and DocuSign Signature Appliance operation. The table also describes the actions and permissions of each of these users.

For more information on how DocuSign Signature Appliance interfaces with Active Directory, refer to [Appendix A: Installation with Reduced Privileges](#).

Table 1 Users Involved in the Installation and Operation of DocuSign Signature Appliance

User	Actions	Active Directory Operations	Permissions	Suggested Permission Group
Domain Administrator	Running the Administrator MMC for performing installation.	Update the Active Directory as follows: Register the DocuSign Signature Appliance as a workstation, and create the following objects: SCP objects, a CA object, a CA AIA object, and a CA CRL object.	Permission to create objects in Active Directory and enable the DocuSign Signature Appliance to update them during operation.	Enterprise admins and Domain admins
Administrator user (name and password are provided during installation)	Registering the DocuSign Signature Appliance as a member of the domain during installation.	Join the DocuSign Signature Appliance to the domain.	Permission to register the appliance as a member of the domain.	Enterprise admins and Domain admins in the domain.
DocuSign Signature Appliance Administrator	Performing administrative operations.	None	Only Active Directory administrators and the built-in administrator can administrate the DocuSign Signature Appliance.	administrators groups in the domain.

Installing DocuSign Signature Appliance in an LDAP based Environment

The solution for LDAP is different from the solution for Microsoft Active Directory. The creation of a new user account is based on a first access performed by the end user. When the user accesses the DocuSign Signature Appliance and presents his/her password, the DocuSign Signature Appliance accesses the LDAP server and presents these credentials. Upon a successful LDAP access, DocuSign Signature Appliance generates a new account for the user and depending on the DocuSign Signature Appliance configuration, generates also a key and a certificate for the end user.

When certain attributes in the user record in the directory are modified (such as the user's email address), a new certificate is generated for the user by the DocuSign Signature Appliance.

When the user is deleted from the directory, the user is also deleted from the DocuSign Signature Appliance and his/her certificate is revoked.

In addition, the DocuSign Signature Appliance also publishes information in the domain, enabling the user to easily access it automatically. For example, it publishes the availability status of the DocuSign Signature Appliance.

The following directories are supported:

- IBM Tivoli.
For more information refer to <http://www.ibm.com/software/tivoli/products/directory-server/>

Note: The identification of the user in the directory is based on the *uid* attribute. The common name of automatically generated user certificates is based on the *givenName* and *sn* attributes.

- SUN Directory Server.
For more information refer to http://www.sun.com/software/products/directory_srvr_ee/dir_srvr/index.xml

Note: The identification of the user in the directory is based on the *uid* attribute. The common name of automatically generated user certificates is based on the *cn* attribute.

- Oracle OID (Oracle Internet Directory).
For more information refer to <http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html>.

Note: The identification of the user in the directory is based on the *uid* attribute. The common name of automatically generated user certificates is based on the *givenName* and *sn* attributes.

Note: The following software installation instructions apply for all Central models, unless otherwise noted.

You install the DocuSign Signature Appliance software from the Administration MMC. In order to manage DocuSign Signature Appliance after installation, you must either be a member of the `administrators` group or be the built-in appliance administrator.

Note: Managing users, groups, and stations are features of the LDAP based directory. The LDAP based directory enables you to define which actions users are permitted to perform. While following this installation procedure, make sure that all user permissions are correctly defined in the Directory, as specified in the procedure.

To install the DocuSign Signature Appliance software:

- Activate the Administration MMC by opening the Start menu and selecting Programs → ARX CoSign → CoSign Control Panel. The Control Panel appears.
- In the Control Panel select Appliances Management. The ARX CoSign Appliance Management window appears.
- Right-click the appliances and select All Tasks → Install → New LDAP appliance. The License Agreement appears.
- Accept the license agreement and click **Next**. The *Network Setup* dialog box appears.

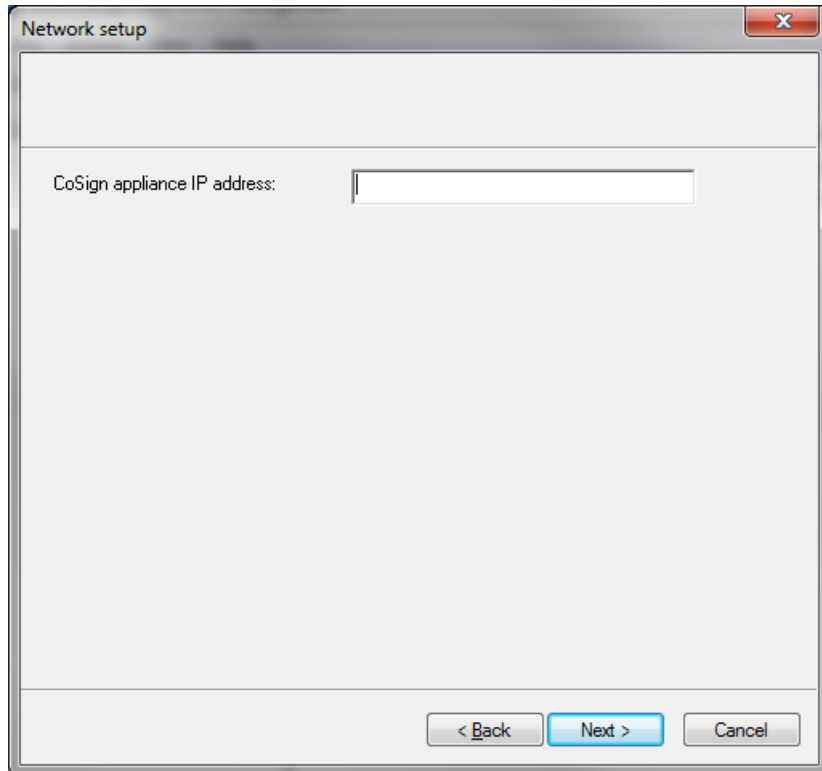


Figure 17 Network Setup Dialog Box

- Enter the **CoSign appliance IP address**. This parameter is necessary for enabling basic communication to and from the DocuSign Signature Appliance. Starting from DocuSign Signature Appliance Hardware version 8.0, IPv6 is also supported. You can enter an IPv6-type IP address in the **CoSign appliance IP address** field.

Note: For information on setting up the IP address of the DocuSign Signature Appliance refer to [Using a Static IP Address](#) and [Enabling DHCP](#).

- Click **Next**. The *CoSign administrator user* dialog box appears.

CoSign administrator user

Enter a user name and a password of a built-in administrator who will manage the CoSign appliance. Do not forget this password, since without remember the password you will not be able to perform important administrative tasks

Admin user name:

Admin password:

Confirm admin password:

< Back Next > Cancel

Figure 18 CoSign Administrator User Dialog Box

- Enter the user name and password of a built-in administrator who will manage the DocuSign Signature Appliance. You will need to enter the password again for confirmation. The built-in administrator is very useful in cases where the LDAP based administrator has a problem connecting to DocuSign Signature Appliance.

Note: Make sure to select an appropriate password for this user since the administrator user name and password that you enter in this dialog box are used for appliance management. During installation, a new user is generated in DocuSign Signature Appliance with this user name and password. In addition, do not forget this password, since without the password you will not be able to perform any administrative task.

- Click **Next**. The *Directory Server Information* dialog box appears

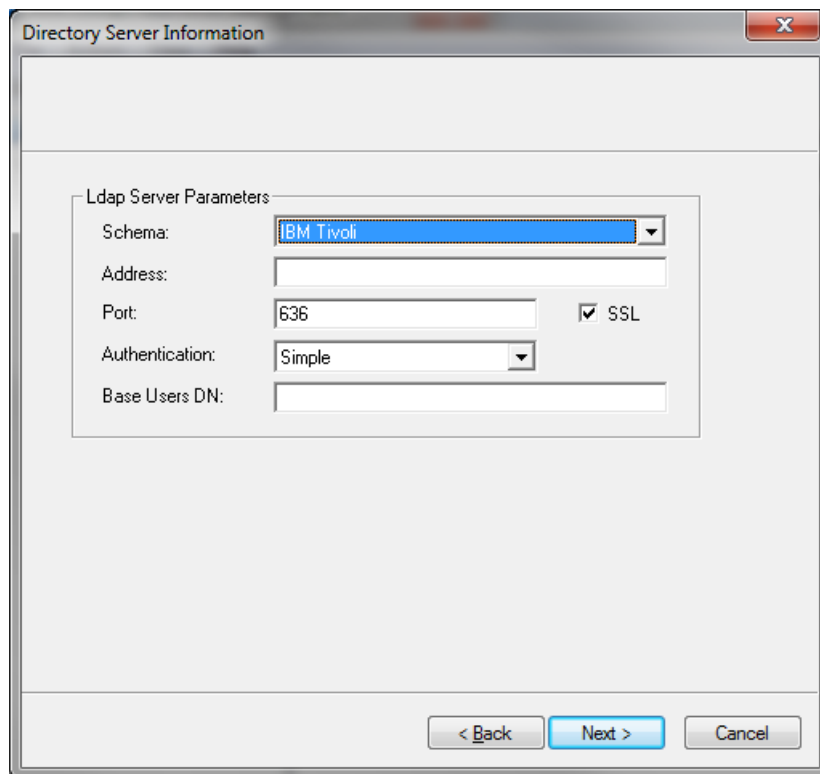


Figure 19 Directory Server Information Dialog Box

- Enter the following information:
 - **Schema** – The commercial name of the LDAP server. This parameter directs DocuSign Signature Appliance to the differences between the LDAP implementations when the DocuSign Signature Appliance interacts with the LDAP Server.
 - **Address** – The DNS name or IP address of the LDAP server.
 - **Port** – The port number of the LDAP server. Usually the port number is 389 or 636 (if LDAP over SSL is used).
 - **SSL** – Select this option if the desired communication between the DocuSign Signature Appliance and the LDAP server is based on SSL.
 - **Authentication** – Select whether the user’s password is transmitted to the LDAP server in the clear or using the digest-MD5 method.
 - **Base Users DN** – The base root of the users tree that determines the scope of users in DocuSign Signature Appliance.
- Click **Next**. The *CA Setup* dialog box appears.

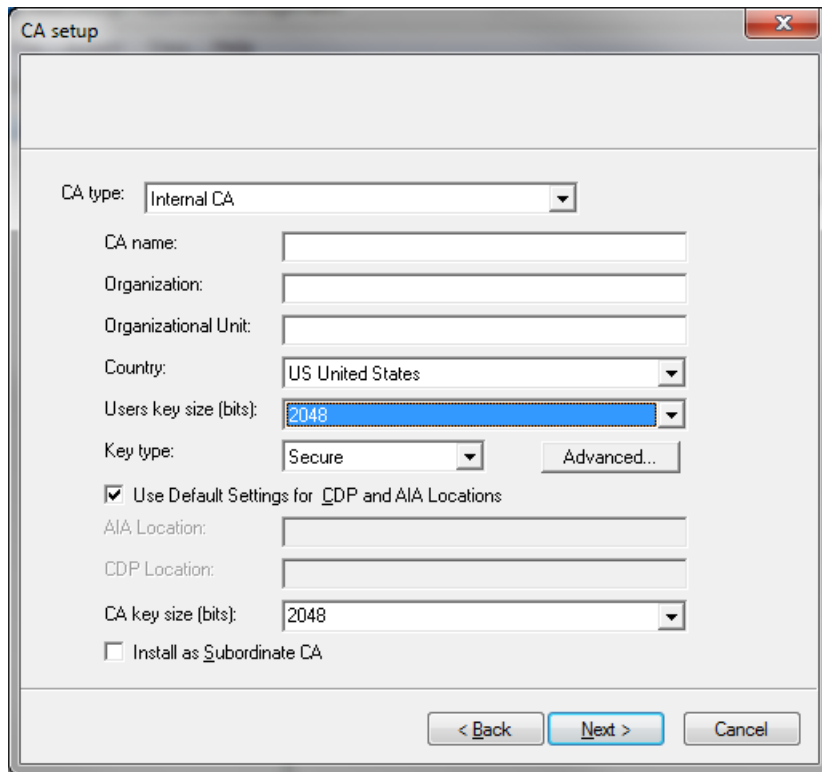


Figure 20 CA Setup Dialog Box

- If you want the DocuSign Signature Appliance to use an internal Certificate Authority (CA) for generating end-user certificates, refer to [Installing an Internal Certificate Authority](#) for detailed explanations of the *CA Setup* dialog box. After setting up the internal CA in the *CA Setup* dialog box, continue with Step [4](#).
- If you want the DocuSign Signature Appliance to use a World Wide Verifiable Certification Authority (CA) for automatically generating end-user certificates, refer to [Using an External World Wide Verifiable CA in Automated Mode](#) for detailed explanations of the *CA Setup* dialog box. After configuring the World Wide verifiable CA in the *CA Setup* dialog box, continue with Step [4](#).
- If you do not wish the DocuSign Signature Appliance to use an internal CA, select the **Without CA** option in the **CA type** drop-down box. It is highly recommended to read the section [Using DocuSign Signature Appliance in Manual External CA Mode](#) before installing DocuSign Signature Appliance with this option.
- Click **Next**. DocuSign Signature Appliance installation begins. A status bar displays the status of the installation operation.

During the installation, status messages appear on both the console display (or on the terminal console, for Central Enterprise) and the Administration MMC display.

- At the **Please insert a backup Minikey** prompt, insert the first backup MiniKey token.
- At the **Please insert a second backup Minikey** prompt, remove the first MiniKey token and insert the second backup MiniKey token.
The second backup MiniKey is a duplicate of the first backup MiniKey.

- At the **Please insert your License Minikey** prompt, insert the license MiniKey token.

If you selected the option **Install as Subordinate CA** in the *CA Setup* dialog box (refer to [Installing an Internal Certificate Authority](#)), several dialog boxes appear, necessitating various operations.

For detailed instructions, go to [Installing DocuSign Signature Appliance as a Subordinate CA](#).

In all other cases, your part in the installation is complete.

- Click **Finish**.

Note: If the first stage of installation was unsuccessful, the DocuSign Signature Appliance returns to its factory settings. This enables you to rerun the installation. In this case, the status bar displays that the installation was unsuccessful, and you can click the **Back** buttons to modify settings before rerunning the installation.

If the installation was unsuccessful and you are unable to rerun the installation, restore DocuSign Signature Appliance to factory settings and then try again.

For more information about restoring factory settings, refer to [Restoring Factory Settings](#).

Note: Clicking **Cancel** does not stop the installation process, it only closes the progress bar on the administration machine (unless you specified a subordinate CA installation).

- In the Administration MMC window, right-click **CoSign appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You can now manage DocuSign Signature Appliance using the Administration MMC (refer to [Chapter 5: Managing the DocuSign Signature Appliance](#)).

Note: Keep the license MiniKey token plugged into the device at all times. Unplugging the license MiniKey for several hours may shut down the service.

Periodically check the number of appliance users. If the number of users is approaching the license limit, contact ARX for a replacement license MiniKey token.

If you received a license with an expiration date, periodically check it using the console to verify it is not about to expire. Refer to [Displaying Status](#) for instructions on how to view the expiration date. Contact ARX for a replacement license MiniKey token before the current key expires.

Note: In a high availability environment, the licenses of all the DocuSign Signature Appliances in the high availability site should have an identical limitation on the number of appliance users.

Note: Store the backup MiniKey in a separate, secure place (e.g., a safe). In case of disaster, you can use the backup MiniKey and the backup file of the DocuSign Signature Appliance's database to safely recover and restore DocuSign Signature Appliance data. For more information on how to backup and restore the DocuSign Signature Appliance's database, refer to [Backing up the DocuSign Signature Appliance Data](#).

If you lose the backup MiniKey, you will not be able to perform some critical functions, such as restoring the DocuSign Signature Appliance (even if you have a backup file), adding an alternate appliance, and performing a reset tamper operation. Therefore, make sure that the backup MiniKey, as well as the second backup MiniKey, will be available when needed.

In Microsoft Active Directory, user keys and certificates are generated during the installation of the DocuSign Signature Appliance. In the case of LDAP based installation, only the administrator account is generated.

A new DocuSign Signature Appliance user is generated when this user attempts to access the DocuSign Signature Appliance. After successfully authenticating the user against the LDAP server, the DocuSign

Signature Appliance generates an account for the user and may generate a key and a certificate for the user, depending on the DocuSign Signature Appliance configuration.

Note: In a Sun One directory installation, you will need to update some system parameters for enabling DocuSign Signature Appliance to access the LDAP based directory. Connect to the appliance administration using the local DocuSign Signature Appliance administrative account. Fill in the parameters **LDAP CoSign User Name** and **LDAP CoSign User Password** with an administrative account that can perform queries to the directory. For more information, refer to [LDAP](#) in [Changing System Parameters](#).

Installing DocuSign Signature Appliance in a Directory Independent Environment

The cases where DocuSign Signature Appliance is installed in a Directory Independent environment fall into two categories:

- DocuSign Signature Appliance is integrated into a product that has its own user management capabilities. User management of the product is not based on Microsoft Active Directory or LDAP.
In this case, DocuSign Signature Appliance provides external signature APIs that enable the integrator to insert a user into DocuSign Signature Appliance upon the creation of a new user in the system. All other user management APIs such as updating a user, deleting a user, etc., are supported through the DocuSign Signature Appliance signature APIs. For information, refer to the *DocuSign Signature Appliance Signature APIs Developer's Guide*.
- DocuSign Signature Appliance is integrated into a product with no user management capabilities. In these cases, the administrator will use a GUI utility to manage the internal DocuSign Signature Appliance users. Refer to [Using the Users Management Utility](#).

To install the DocuSign Signature Appliance software:

- Activate the Administration MMC by opening the **Start** menu and selecting **Programs → ARX CoSign → CoSign Control Panel**. The Control Panel appears.
- In the Control Panel select **Appliances Management**. The *ARX CoSign Appliance Management* window appears.
- Right-click **appliances** and select **All Tasks → Install → New Directory Independent appliance**. The License Agreement appears.
- Accept the license agreement and click **Next**. The *Network Setup* dialog box appears.

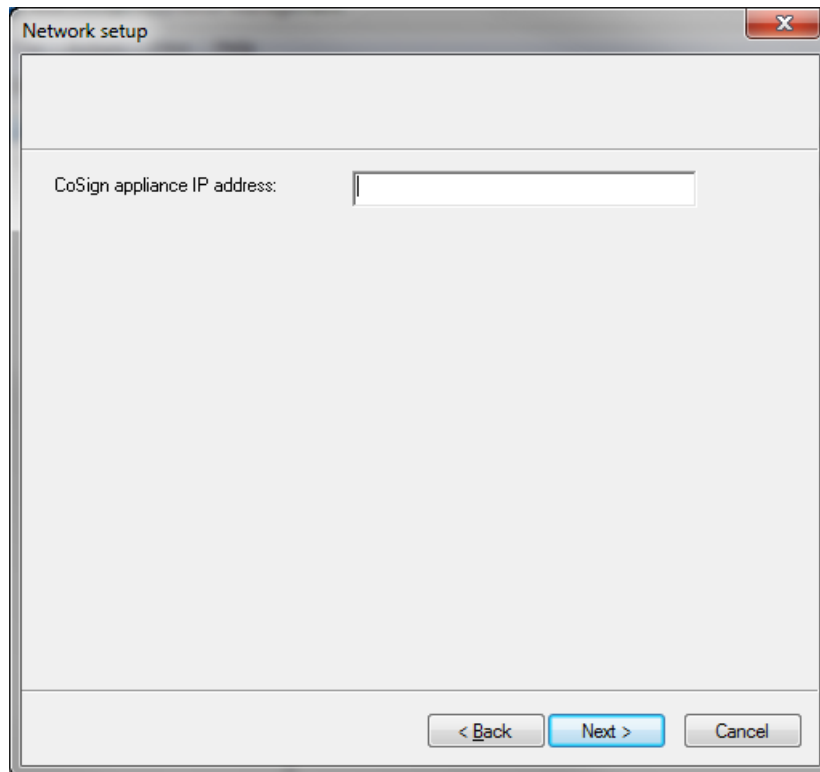
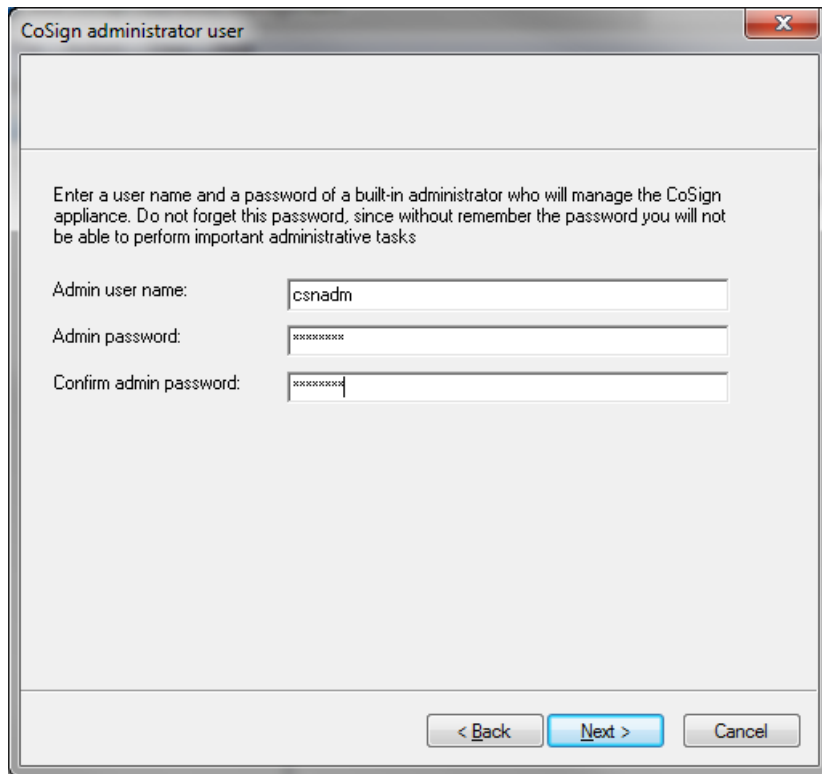


Figure 21 Network Setup Dialog Box

- Enter the **CoSign appliance IP address**. This parameter is necessary for enabling basic communication to and from the DocuSign Signature Appliance. Starting from DocuSign Signature Appliance Hardware version 8.0, IPv6 is also supported. You can enter an IPv6-type IP address in the **CoSign appliance IP address** field.

Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to [Using a Static IP Address](#) and [Enabling DHCP](#).

- Click **Next**. The *CoSign Administrator User* dialog box appears.



The image shows a dialog box titled "CoSign administrator user". It contains a warning message: "Enter a user name and a password of a built-in administrator who will manage the CoSign appliance. Do not forget this password, since without remember the password you will not be able to perform important administrative tasks". Below the message are three input fields: "Admin user name:" with the value "csnadm", "Admin password:" with masked characters, and "Confirm admin password:" with masked characters. At the bottom are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

Figure 22 CoSign Administrator User Dialog Box

- Enter the **CoSign Admin user name** and **Admin password**, then enter the password again for confirmation. This user will perform the administrative tasks.

Note: Make sure to select an appropriate password for this user since the administrator user name and password that you enter in this dialog box are used for the appliance management. During installation, a new user is generated in DocuSign Signature Appliance with this user name and password.

- Click **Next**. The *CA Setup* dialog box appears.

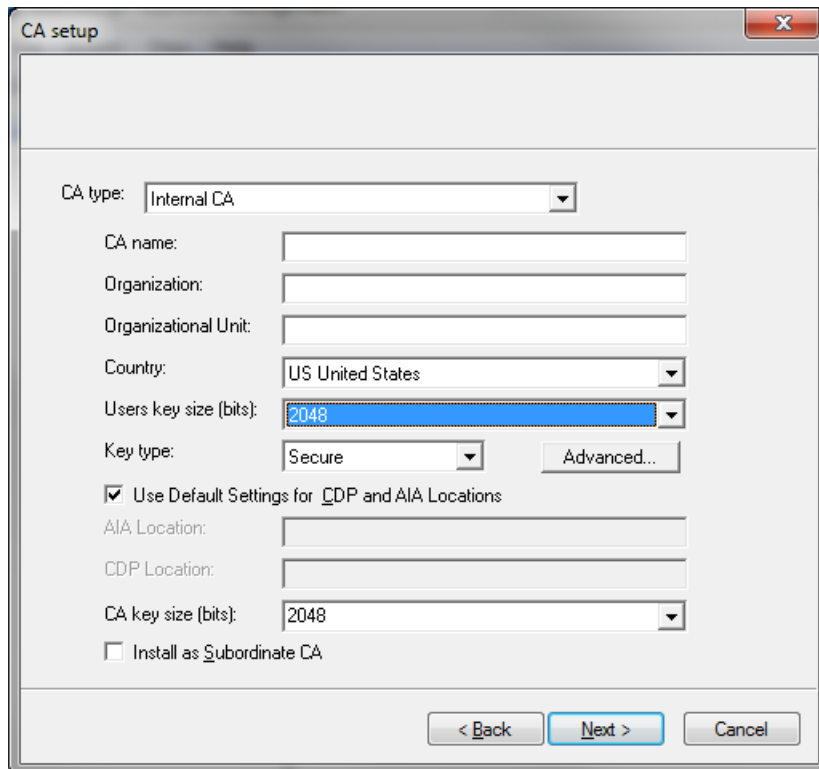


Figure 23 CA Setup Dialog Box

- If you want the DocuSign Signature Appliance to use an internal Certificate Authority (CA) for generating end-user certificates, refer to [Installing an Internal Certificate Authority](#) for detailed explanations of the CA Setup dialog box. After setting up the internal CA in the CA Setup dialog box, continue with Step 4.
- If you want the DocuSign Signature Appliance to use a World Wide Verifiable Certification Authority (CA) for automatically generating end-user certificates, refer to [Using an External World Wide Verifiable CA in Automated Mode](#) for detailed explanations of the CA Setup dialog box. After configuring the World Wide verifiable CA in the CA Setup dialog box, continue with Step 4.
- If you do not wish the DocuSign Signature Appliance to use an internal CA, select the **Without CA** option in the **CA type** drop-down box. It is highly recommended to read the section [Using DocuSign Signature Appliance in Manual External CA Mode](#) before installing DocuSign Signature Appliance with this option.
- Click **Next**. DocuSign Signature Appliance installation begins. A status bar displays the status of the installation operation.

During the installation, status messages appear on both the console display (or on the terminal console, for Central Enterprise) and the Administration MMC display.

- At the **Please insert a backup Minikey** prompt, insert the first backup MiniKey token.
- At the **Please insert a second backup Minikey** prompt, remove the first MiniKey token and insert the second backup MiniKey token.
The second backup MiniKey is a duplicate of the first backup MiniKey.

- At the **Please insert your License Minikey** prompt, insert the license MiniKey token.
If you selected the option **Install as Subordinate CA** in the *CA Setup* dialog box (refer to [Installing an Internal Certificate Authority](#)), several dialog boxes appear, necessitating various operations. For detailed instructions, refer to [Installing DocuSign Signature Appliance as a Subordinate CA](#).

In all other cases, your part in the installation is complete.

- Click **Finish**.

Note: If the first stage of installation was unsuccessful, the DocuSign Signature Appliance returns to its factory settings. This enables you to rerun the installation. In this case, the status bar displays that the installation was unsuccessful, and you can click the **Back** buttons to modify settings before rerunning the installation.

If the installation was unsuccessful and you are unable to rerun the installation, restore DocuSign Signature Appliance to factory settings and then try again.

For more information about restoring factory settings, refer to [Restoring Factory Settings](#).

Note: Clicking **Cancel** does not stop the installation process, it only closes the progress bar on the administration machine (unless you specified a subordinate CA installation).

- In the Administration MMC window, right-click **CoSign appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You can now manage DocuSign Signature Appliance using the Administration MMC (refer to [Chapter 5: Managing the DocuSign Signature Appliance](#)).
- Activate the ARX *Users Management* utility to add users and automatically generate keys and certificates for these users (refer to [Using the Users Management Utility](#)).

The created DocuSign Signature Appliance users can connect to DocuSign Signature Appliance and perform digital signature operations.

Note: Keep the license MiniKey token plugged into the device at all times. Unplugging the license MiniKey for several hours may shut down the service.

Periodically check the number of appliance users. If the number of users is approaching the license limit, contact ARX for upgrading the license MiniKey token.

If you received a license with an expiration date, periodically check it using the console to verify it is not about to expire. Refer to *Displaying Status* for instructions on how to view the expiration date. Contact ARX for a replacement license MiniKey token before the current key expires.

Note: In a high availability environment, the licenses of all the DocuSign Signature Appliances in the high availability site should have an identical limitation on the number of appliance users.

Note: Store the backup MiniKey in a separate, secure place (e.g., a safe). In case of disaster, you can use the backup MiniKey and the backup file of the DocuSign Signature Appliance's database to safely recover and restore DocuSign Signature Appliance data. For more information on how to backup and restore the DocuSign Signature Appliance's database, refer to [Backing up the DocuSign Signature Appliance Data](#).

If you lose the backup MiniKey, you will not be able to perform some critical functions, such as restoring the DocuSign Signature Appliance (even if you have a backup file), adding an alternate

appliance, and performing a reset tamper operation. Therefore, make sure that the backup MiniKey, as well as the second backup MiniKey, will be available when needed.

Installing DocuSign Signature Appliance in a Common Criteria EAL4+ Mode as a Signature Creation Device or Seal Creation Device

The installation is similar to installing DocuSign Signature Appliance in Directory Independent mode.

To install the DocuSign Signature Appliance software:

- Activate the Administration MMC by opening the **Start** menu and selecting **Programs** → **ARX CoSign** → **CoSign Control Panel**. The Control Panel appears.
- In the Control Panel select **Appliances Management**. The *ARX CoSign Appliance Management* window appears.
- Right-click **appliances** and select **All Tasks** → **Install** → **New Common Criteria appliance**. The License Agreement appears.
- Accept the license agreement and click **Next**. The *Network Setup* dialog box appears.

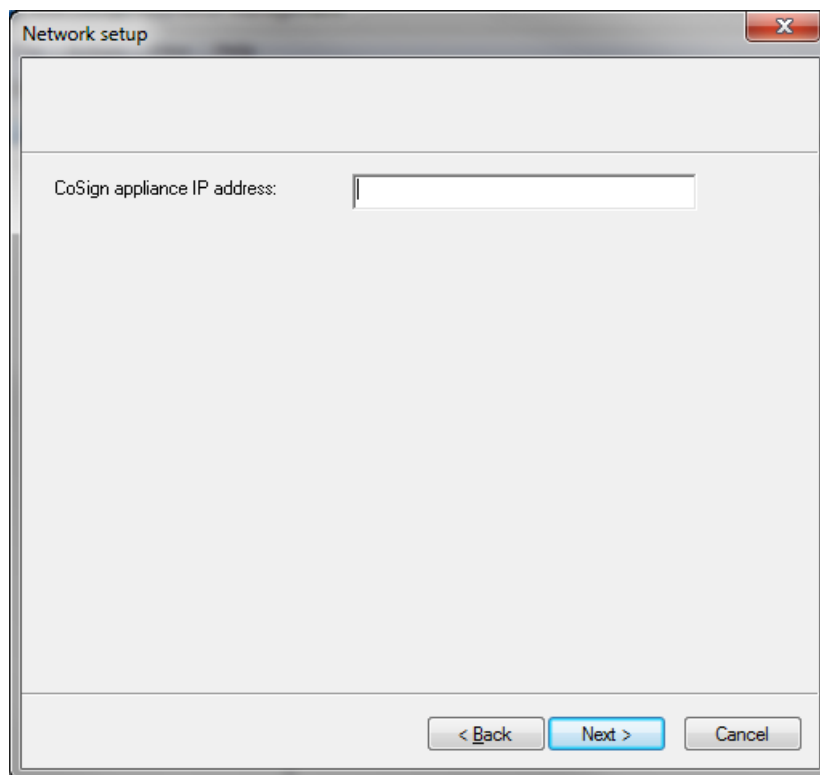


Figure 24 Network Setup Dialog Box

- Enter the **CoSign appliance IP address**. This parameter is necessary for enabling basic communication to and from the DocuSign Signature Appliance. Starting from DocuSign Signature Appliance Hardware version 8.0, IPv6 is also supported. You can enter an IPv6-type IP address in the **CoSign appliance IP address** field.

Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to [Using a Static IP Address](#) and [Enabling DHCP](#).

- Click **Next**. The *CoSign Administrator User* dialog box appears.

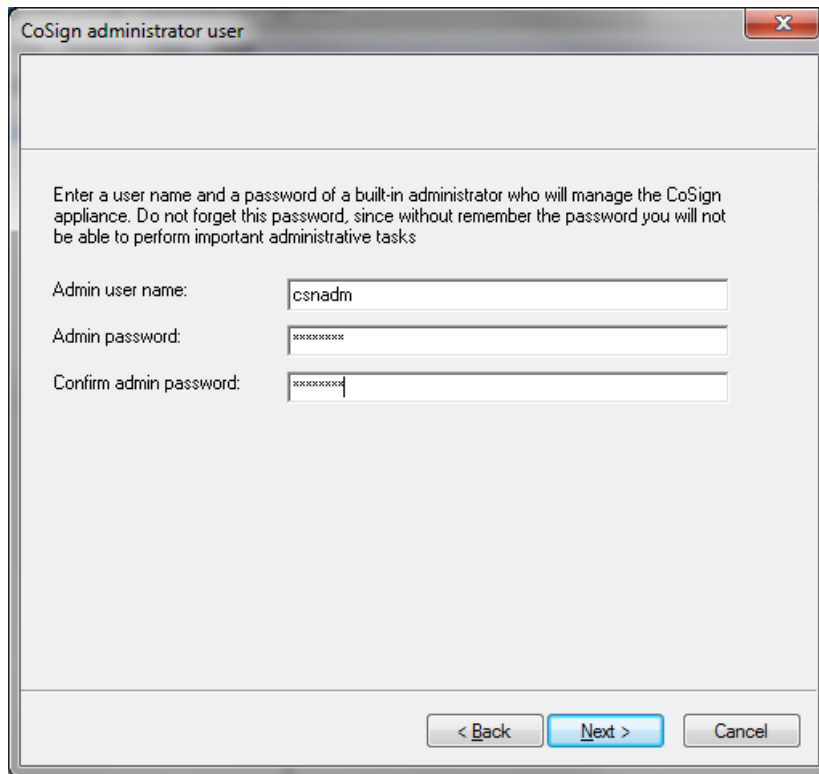


Figure 25 CoSign Administrator User Dialog Box

- Enter the **CoSign Admin user name** and **Admin password**, then enter the password again for confirmation. This user will perform the administrative tasks.

Note: Make sure to select an appropriate password for this user since the administrator user name and password that you enter in this dialog box are used for the appliance management. During installation, a new user is generated in DocuSign Signature Appliance with this user name and password.

- Click **Next**. DocuSign Signature Appliance installation begins. A status bar displays the status of the installation operation.

During the installation, status messages appear on both the console display and the Administration MMC display.

- At the **Please insert a backup Minikey** prompt, insert the first backup MiniKey token.
- At the **Please insert a second backup Minikey** prompt, remove the first MiniKey token and insert the second backup MiniKey token.
The second backup MiniKey is a duplicate of the first backup MiniKey.
- At the **Please insert your License Minikey** prompt, insert the license MiniKey token.

Your part in the installation is complete.

- Click **Finish**.

Note: If the first stage of installation was unsuccessful, the DocuSign Signature Appliance returns to its factory settings. This enables you to rerun the installation. In this case, the status bar displays that the installation was unsuccessful, and you can click the **Back** buttons to modify settings before rerunning the installation.

If the installation was unsuccessful and you are unable to rerun the installation, restore DocuSign Signature Appliance to factory settings and then try again.

For more information about restoring factory settings, refer to [Restoring Factory Settings](#).

Note: Clicking **Cancel** does not stop the installation process, it only closes the progress bar on the administration machine (unless you specified a subordinate CA installation).

- In the Administration MMC window, right-click **CoSign appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You can now manage DocuSign Signature Appliance using the Administration MMC (refer to [Chapter 5: Managing the DocuSign Signature Appliance](#)).
- Activate the ARX `Users Management` utility to add users and automatically generate keys and certificates for these users (refer to [Using the Users Management Utility](#)).

The created DocuSign Signature Appliance users can connect to DocuSign Signature Appliance and perform digital signature operations.

Note: Keep the license MiniKey token plugged into the device at all times. Unplugging the license MiniKey for several hours may shut down the service.

Periodically check the number of appliance users. If the number of users is approaching the license limit, contact ARX for upgrading the license MiniKey token.

If you received a license with an expiration date, periodically check it using the console to verify it is not about to expire. Refer to [Displaying Status](#) for instructions on how to view the expiration date. Contact ARX for a replacement license MiniKey token before the current key expires.

Note: In a high availability environment, the licenses of all the DocuSign Signature Appliance appliances in the high availability site should have an identical limitation on the number of appliance users.

Note: Store the backup MiniKey in a separate, secure place (e.g., a safe).

If you lose the backup MiniKey, you will not be able to perform some critical functions, such as adding an alternate appliance, and performing a reset tamper operation. Therefore, make sure that the backup MiniKey, as well as the second backup MiniKey, will be available when needed.

Installing an Internal Certificate Authority

The *CA Setup* dialog box appears during the course of the software installation. It enables setting up the DocuSign Signature Appliance to use an internal Certificate Authority (CA) for generating end-user keys and certificates. This section describes in detail the various options available in the dialog box.

Figure 26 CA Setup Dialog Box

To specify an Internal CA:

- Specify **Internal CA** in the **CA type** field.
- Enter the following information:
 - **CA name** – The identifying name of DocuSign Signature Appliance’s internal CA. This name will also be displayed as the **Issuer Name** in the certificates issued by the DocuSign Signature Appliance.
 - **Organization** – The CA’s organization. This field is included in the CA’s certificate. This field is optional.
 - **Organizational Unit** – The organizational unit of the CA. This field is included in the CA’s certificate. This field is optional.

Note: The Organizational Unit parameter in the certificate does not have to be identical with the **Users Container** field in the Microsoft Active Directory, which is provided during the Directory Setup (Figure 14).

- **Country** – The CA’s country. This field is included in the CA’s certificate.
- **Users key size (bits)** – The size, in bits, of the end-users’ generated keys. Bigger RSA keys result in larger digital signatures and higher security. However, this results in slower overall performance. Currently, the maximum user key size is 4096 bits.
- **Key type** – The default Key Type is *Secure*.

- **Use Default Settings for CDP and AIA Locations** – Select whether to use the default settings for the AIA (Authority Information Access) and CDP (CRL Distribution Point) locations. If you choose not to use the default settings, enter the desired settings:

- **AIA Location** – AIA (Authority Information Access) is put into the end user's certificate and specifies where the CA certificate is located in the organization's network.

The AIA can be accessed using the HTTP protocol, LDAP protocol, a file in the organization's network, or a local file in the end user's hard disk.

The value entered in this field will be included in every end user's certificate that is generated by DocuSign Signature Appliance.

Deselecting the **Use Default Settings for CDP and AIA Locations** option while leaving this entry empty, triggers a null AIA in the end user's certificate.

The default value in the case of Active Directory includes the LDAP location. If the default is not modified, the DocuSign Signature Appliance installation will also put the ROOT certificate in the proper LDAP location.

In a Directory Independent environment, the default is an empty entry.

If the administrator decides to change the AIA default value, the administrator must place the CA certificate in the location specified in the AIA. In addition, whenever the CA certificate is renewed, the administrator must place it in the location specified in the AIA.

- **CDP Location** – CDP (CRL Distribution Point) is put into the end user's certificate and specifies where the CA's CRL (Certificate Revocation List) is located in the organization's network.

The CDP can be accessed using the HTTP protocol, LDAP protocol, a file in the organization's network, or a local file in the end user's hard disk.

The value entered in this field will be included in every end user's certificate that is generated by the DocuSign Signature Appliance.

Deselecting the **Use Default Settings for CDP and AIA Locations** option while leaving this entry empty, triggers a null CDP in the end user certificate.

The default value in the case of Active Directory includes the LDAP location. If the default is not modified, DocuSign Signature Appliance will constantly update the CDP with the updated CRL.

In a Directory Independent environment, the default is an empty entry.

If the administrator decides to change the CDP default value, the administrator must place the CRL in the location specified in the CDP.

For details on obtaining the DocuSign Signature Appliance AIA and CRL, refer to [Changing System Parameters](#).

- **CA key size (bits)** – The size of the key of the CA.
- **Install as Subordinate CA** – Select this option if you wish to install the CA as a subordinate CA.

You can install the CA as a subordinate CA of another CA (who can be a subordinate CA of another CA, etc.). This option is useful if you are installing DocuSign Signature Appliance in an organization with an existing CA or in cases where a national CA certifies organizational CAs, and you wish to integrate into the existing infrastructure.

Note: Selecting the **Install as Subordinate CA** option will necessitate performing various tasks before installation is complete. These tasks are described in detail in [Installing DocuSign Signature Appliance as a Subordinate CA](#).

After completing CA Setup, return to the software installation procedure as follows:

- If you are installing DocuSign Signature Appliance in a Microsoft Active Directory Environment, continue with Step [4](#).
- If you are installing DocuSign Signature Appliance in an LDAP based Environment, continue with Step [4](#).
- If you are installing DocuSign Signature Appliance in a Directory Independent Environment, continue with Step [4](#).

Advanced Settings

The **Advanced** option available from the *CA Setup* dialog box enables the administrator to control additional configuration parameters used by the DocuSign Signature Appliance installation. These parameters enable sending email notifications to end users during and after installation, and defining SSL proxy parameters that are relevant when DocuSign Signature Appliance is configured to use a Worldwide Verifiable External CA in automated mode.

Figure 27 Advanced Settings Dialog Box

- **Enable Email Notification** – Check this option to direct DocuSign Signature Appliance to send email notifications to end users. Enter the following information:
 - ◆ **Mail server name** – IP address or DNS name of the organization’s mail server.

- ◆ **Mail server port** – The port number of the organization’s mail server.
- ◆ **Email from address** – The address from which to send email notifications to users.
- **Enable the server to use proxy for internet access** – check this option to enable DocuSign Signature Appliance to communicate with the internet through an SSL proxy. This option is relevant for cases where DocuSign Signature Appliance is configured to use a Worldwide Verifiable CA in automatic mode, and the organization communicates via the Internet through an SSL proxy.
You can use proxies that require a user name and password authentication before communicating with the external HTTPS server.
 - ◆ **Proxy’s address** – The IP address or DNS name of the organization’s SSL proxy.
 - ◆ **Port** – The port number of the organization’s SSL proxy.
 - ◆ **User name** – The identity of the user being verified by the proxy.
 - ◆ **User password** – The password of the user being verified by the proxy.

Using an External CA in Manual Mode

This CA mode is the only available CA mode if DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.

If DocuSign Signature Appliance is installed in an environment where an external CA is used in manual mode, the DocuSign Signature Appliance will generate an empty account for the signing users, but will not generate signature keys or certificates.

Each authenticated user of the appliance will need to manually enroll for a certificate. The certificate generation process is as follows:

- The user communicates with the certificate enrollment pages of the CA using client tools that are executed in the end-user’s PC. One example of such a tool is a regular browser.
You can optionally use tools that are developed using SAPI or RESTful API.
- During enrollment, a command to generate a key is sent from the DocuSign Signature Appliance client to the DocuSign Signature Appliance. The DocuSign Signature Appliance securely generates a signature key for the user, and a certificate request is sent by the DocuSign Signature Appliance client to the external CA using the CA interface. The CA interface is usually a web-based interface.
- The external CA generates a certificate and sends it to the user.
- The user imports the certificate to the DocuSign Signature Appliance using the CA application. This is usually a web-based application.
You can optionally use tools that are developed using SAPI or RESTful API.

After the certificate is uploaded to the DocuSign Signature Appliance, the user can sign normally using the newly uploaded certificate.

In this mode of work, the user must repeat this procedure upon certificate renewal.

Note: In a Common Criteria EAL4+ mode of operation, the user is required to activate his/her account prior to any operation, including key and certificate enrollment as well as signing with the generated signature key. For information on how to activate an account, refer to [Performing User Activation](#).

Using an External World Wide Verifiable CA in Automated Mode

The *CA Setup* dialog box appears during the course of DocuSign Signature Appliance software installation. It enables setting up the DocuSign Signature Appliance to use an external CA whose ROOT certificate is automatically installed in many workstations.

In this way, a document that is signed using DocuSign Signature Appliance can be properly verified without having to install ROOT certificate in all third-party workstations that need to verify the signature of the document.

In this work mode, the end user's keys are generated inside the DocuSign Signature Appliance.

Immediately after the key is generated, a certificate request is sent to the external CA. The external CA replies with the user certificate.

After the certificate is returned to the DocuSign Signature Appliance from the external CA, the end user can start signing documents.

The Comodo World Wide Verifiable CA is available in automated mode.

The following section explains how to use the Comodo external World Wide Verifiable CA.

Using an External World Wide Verifiable CA in Automated Mode - Comodo

The *CA Setup* dialog box appears during the course of DocuSign Signature Appliance software installation. It enables setting Comodo as the external World Wide Verifiable CA in automated mode.

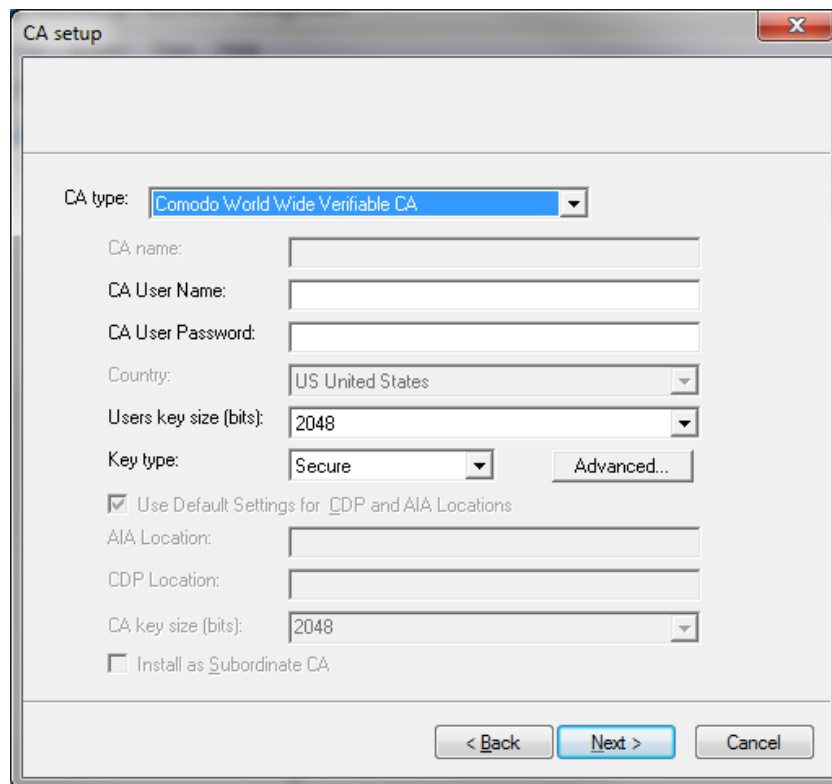


Figure 28 CA Setup – Comodo World Wide Verifiable CA Dialog Box

To specify the Comodo World Wide Verifiable CA:

- Specify **Comodo World Wide Verifiable CA** in the **CA type** field.
- Enter the following information:

- **CA User Name** – Contact ARX for a special user ID for communication with the external CA.
- **CA User Password** – Contact ARX for a password for authenticating the organization to the external CA.
- **Users key size (bits)** – The size, in bits, of the end-users' generated keys. Bigger RSA keys result in larger digital signatures and higher security. However, this results in slower overall performance. Currently, the maximum user key size is 4096 bits, and the minimum user key size is 2048 bits.
- **Key type** – The default Key Type is *Secure*.
After completing CA Setup, return to the software installation procedure as follows:
 - If you are installing DocuSign Signature Appliance in a Microsoft Active Directory Environment, continue with Step [4](#).
 - If you are installing DocuSign Signature Appliance in an LDAP based Environment, continue with Step [4](#).
 - If you are installing DocuSign Signature Appliance in a Directory Independent Environment, continue with Step [4](#).

Installing DocuSign Signature Appliance as a Subordinate CA

This section applies to users who selected the option **Install as Subordinate CA** in the *CA Setup* dialog box (refer to [Installing an Internal Certificate Authority](#)). The sections describing the software installation process in each of the three environments (Active Directory, LDAP, and Directory Independent) refer you to this section just before the end of the installation process, after inserting the license MiniKey token.

You are prompted to perform the following tasks, after which DocuSign Signature Appliance installation is complete:

- A *File Selection* dialog box appears, prompting you to supply the name of the file that will contain the Certificate Request (CRQ) that should be submitted to the ROOT CA.
Prior to this step, the DocuSign Signature Appliance internally generated a key for the CA, and then created a certificate request based on the generated key.
DocuSign Signature Appliance then exported the CRQ that should be sent to the ROOT CA.
- Specify the name of the CRQ file.

The *Subordinate CA Installation* dialog box appears:

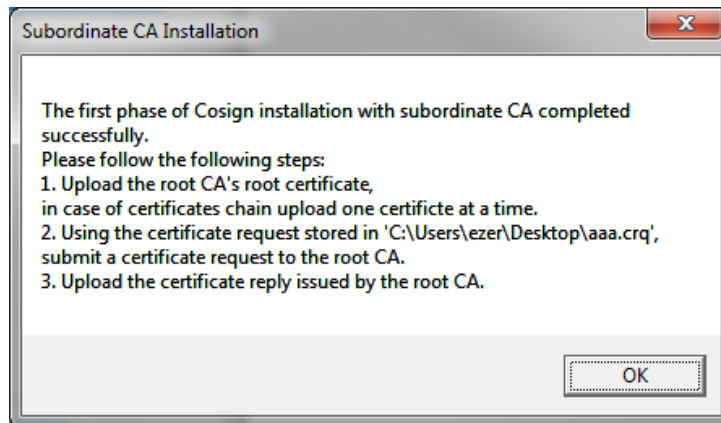


Figure 29 Subordinate CA Installation Dialog Box

The *Subordinate CA Installation* dialog box lists the tasks you still need to perform before DocuSign Signature Appliance users can be created. The following steps describe those tasks.

- Exit the Administration MMC.
- Submit the Certificate Request to the ROOT CA by providing the CRQ file.

The files you will eventually receive back from the ROOT CA include a group of files that constitute the complete chain of CA certificates, and the Certificate Reply file that contains the new subordinate CA certificate. The subordinate CA certificate can also be packaged in certificate format (.cer) and not necessarily in a certificate reply format (.crp).

Note that if a ROOT CA certified DocuSign Signature Appliance, the complete chain of CA certificates includes only the ROOT CA certificate.

Note: Make sure that the certificate reply contains only the DocuSign Signature Appliance certificate and does not contain any of the certificates that are part of the certificate chain. The certificates in the certificate chain are loaded separately.

Note: The file formats of the certificate and certificate chain must be ASN.1(DER) encoded. If the files are encoded in BASE64 format, they must be converted. If the DocuSign Signature Appliance subordinate CA certificate is encoded in BASE64 format, you can use the Microsoft standard certificate information utility to browse to that BASE64 certificate, and use the *copy to file* option to save the certificate to a DER encoded certificate.

- Once you receive the files from the ROOT CA, activate the Administration MMC by opening the **Start** menu and selecting **Programs** → **ARX CoSign** → **CoSign Control Panel**. Select **Appliances Management**, and the *ARX CoSign Appliance Management* window appears.
- For each file in the chain of CA certificates, perform the following:
 - Right-click the relevant **appliance** and select **All Tasks** → **Subordinate CA** → **Load ROOT Cert Chain**.

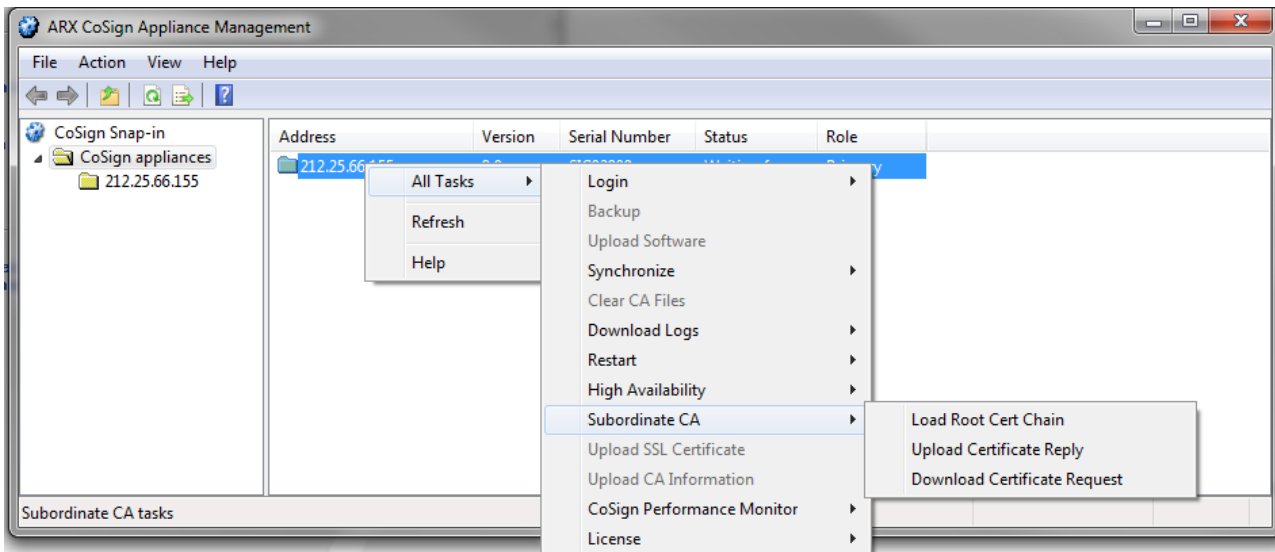


Figure 30 Subordinate CA Installation – Loading the CA Certificates

A file selection window pops up.

- Specify the path and file name of the CA certificate.

After each certificate is loaded, the following message appears: **Uploading root certificate chain finished successfully.**

- Right-click **appliances** and select **All Tasks** → **Subordinate CA** → **Upload Certificate Reply**.

A dialog box appears, prompting you to specify the Certificate Reply file, which contains the new subordinate CA certificate.

- Specify the path and file name of the Certificate Reply.

A message appears: **Waiting for the CA service to restart...** and soon after DocuSign Signature Appliance proceeds with the installation process. In an Active Directory, DocuSign Signature Appliance now automatically creates DocuSign Signature Appliance users and generates keys and certificates for them. In a Directory Independent environment, you must activate the `Users Management` utility to create DocuSign Signature Appliance users and generate keys and certificates for them (refer to [Using the Users Management Utility](#)).

Note: In an LDAP environment or Active Directory multiple domain environment, a new account is generated when the end user first attempts to connect to DocuSign Signature Appliance.

At the end, the following message is displayed: **Uploading certificate reply finished successfully.**

The created DocuSign Signature Appliance users can now connect to DocuSign Signature Appliance and perform digital signature operations.

Note: Keep in mind that setting up DocuSign Signature Appliance as a subordinate CA requires further administrative attention. The subordinate CA certificate should be renewed according to the ROOT CA policy. It is recommended to start the renewal process a month before certificate expiration.

Multi-Language Support

You can deploy DocuSign Signature Appliance in environments that allow the use of non-ASCII characters in fields such as the user's common name in the certificate, etc.

However, due to system limitations, there are cases where multi-language environments cannot be supported. For more information about these limitations, refer to the DocuSign Signature Appliance release notes.

Chapter 4: Deploying the DocuSign Signature Appliance Client

This chapter describes how to:

- Deploy the DocuSign Signature Appliance Client, in a Microsoft-Active Directory environment, LDAP based environment, or a Directory Independent environment.
- Use the Control Panel.
- Use the graphical signature management application that enables setting a graphical signature for users of the organization.
- Install the ROOT certificate to validate DocuSign Signature Appliance signatures in an organization without DocuSign Signature Appliance.
- Use CoSign Verifier to validate digital signatures that were attached to Microsoft Office documents using DocuSign Signature Appliance.

Note: The installation of DocuSign Signature Appliance differs slightly depending on whether it is being installed in a Microsoft Active Directory environment, LDAP based environment, or Directory Independent environment. These differences are mentioned where applicable.

Deploying the Client

DocuSign Signature Appliance enables the end-user to digitally sign transactions, documents, and other types of data. In order to perform these tasks, the DocuSign Signature Appliance client must be installed. The DocuSign Signature Appliance client enables applications (e.g., Microsoft Word) to use DocuSign Signature Appliance for generating digital signatures. For more information on generating signatures in third-party applications, refer to the *DocuSign Signature Appliance Client User Guide*.

The DocuSign Signature Appliance client may be installed on a machine using one of the following operating systems:

- Windows 2008/Windows 2008-R2
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2012

Note: The DocuSign Signature Appliance client can be also be installed in any 64 bit variant of the above operating systems, such as Windows 7 64 bit.

Deployment Options

The DocuSign Signature Appliance client can be deployed on an end-user machine, a terminal server, a Web server, or application server.

On an End-User Machine

Deploying the client on an end-user machine enables end-users to use DocuSign Signature Appliance for generating digital signatures on documents, transactions, or other types of data. Each client installation generally services one end-user.

On a Terminal Server

Deploying the client on a terminal server (e.g., Citrix Server or Microsoft Terminal Server) enables multiple users to concurrently use DocuSign Signature Appliance for signing and validating signatures. This circumvents the need to install the client on each end-user's machine.

End-users connect to the terminal server and use the installed applications (e.g., Microsoft Word or Outlook) remotely. If the end-user wishes to sign a document, the signature is attached in the terminal server via the installed DocuSign Signature Appliance client.

On a Web Server or Application Server

You can deploy the DocuSign Signature Appliance client on a Web server. This enables multiple end-users to use DocuSign Signature Appliance for generating signatures in Web applications without deploying the client on every end-user's machine, and without requiring the end-user machines to be part of the domain.

ARX provides digital signature APIs through a C/C++ interface or COM interface. These Signature APIs are explained in detail in the *DocuSign Signature Appliance Signature APIs Developer's Guide*. When the end-user wants to add a digital signature, the Web application prompts the end-user for a login name and password. Through DocuSign Signature Appliance's SAPI COM interface, the Web server creates a signature using DocuSign Signature Appliance by providing the end user's credentials (User ID, password, and domain name). The digital signature value can then be attached to the signed data by the Web application.

In addition, a web server can use DocuSign Signature Appliance through a Web Services interface, which is executed in the DocuSign Signature Appliance. An additional Web Services interface that is based on a RESTful API can optionally be used.

For more information, refer to the *DocuSign Signature Appliance Signature APIs Developer's Guide*.

The DocuSign Signature Appliance client can also be installed on a Microsoft SharePoint server. For more information, refer to the *Connector for SharePoint User Guide*.

The DocuSign Signature Appliance client can also be installed together with a Web App deployment on a Microsoft web server. For more information, refer to the *Web App User Guide*.

Installing the DocuSign Signature Appliance Client

The DocuSign Signature Appliance Client can either be installed directly from the ARX CoSign CD or automatically using a centralized mechanism. Regardless of how the client is deployed, the client must be installed on the appropriate machine with all the relevant plug-ins.

Note: You must have local administrative rights in order to install the DocuSign Signature Appliance client.

Note: If the internal CA is used for generating end user's certificates, then for all environments except Microsoft Active Directory, the ROOT certificate must be manually installed on every workstation on

which a DocuSign Signature Appliance client is installed. Refer to the section *Installing the Root Certificate and CoSign Verifier* in the *DocuSign Signature Appliance Client User Guide*.

DocuSign Signature Appliance Client Components

The DocuSign Signature Appliance Client CD displays a *CoSign Client Components Installation* screen when the DocuSign Signature Appliance Client CD is inserted into the CD driver.

Each DocuSign Signature Appliance component is based on several .msi files. The .msi files are based on the Microsoft Software Installation technology.

The components include:

- ARX DocuSign Signature Appliance Client – The standard DocuSign Signature Appliance client installation without any plug-ins. The installation includes the following .msi files:
 - ARX CryptoKit – Provides the basic standard Cryptographic APIs, which include PKCS#11 and MS-CAPI. These API enable off-the shelf products, such as MS Outlook and MS Office 2010/2013/2016, to use DocuSign Signature Appliance without any integration efforts. For more information about ARX CryptoKit, refer to the ARX CryptoKit documentation. The CryptoKit installation file name is ARX CryptoKit Basic.msi. The 64 bit CryptoKit installation file name is ARX CryptoKit Basic64.msi.
 - ARX DocuSign Signature Appliance Client.msi – Provides the basic functionality for interfacing with the DocuSign Signature Appliance. The DocuSign Signature Appliance client installation file name for 64 bit operating systems is ARX DocuSign Signature Appliance Client64.msi.
 - ARX Signature API.msi – Provides signature APIs for enabling OEMs to use DocuSign Signature Appliance with a minimal development effort. The APIs also include a COM-based interface that enables applications to use DocuSign Signature Appliance. The Signature API installation file name for 64 bit operating systems is ARX Signature API64.msi. For more information about the Signature API, refer to the *DocuSign Signature Appliance Programmers Guide*.
- ARX DocuSign Signature Appliance admin – Enables administrators to install and manage DocuSign Signature Appliance. The installation and management activities are described in [Chapter 3: Installing DocuSign Signature Appliance](#) and [Chapter 6: Using the Consoles](#). The ARX DocuSign Signature Appliance admin component is based on the following .msi files:
 - ARX DocuSign Signature Appliance Admin Client.msi – Includes all the administrative components of DocuSign Signature Appliance. For example, it includes the Administration MMC for managing the DocuSign Signature Appliance.
 - ARX Signature PAD.msi – Includes all the software necessary for installation of the graphical signature pad and the utility that controls the pad. For more information, refer to [Using the Graphical Signature Management Application](#).
- Microsoft Office (Word, Excel) – Two types of plug-ins are supported:

- ARX Signature Line Provider – A digital signature plug-in for Office 2010/2013/2016 for the .docx and .xlsx file types.
- ARX Legacy Word Add-in – A digital signature plug-in for Word 2010/2013/2016 and Excel 2010/2013/2016 that enables you to sign .doc and .xls files.

For more information, refer to Signing Microsoft Office Documents in the DocuSign Signature Appliance Client User Guide.

- ARX OmniSign Printer – A plug-in for signing any printable data from any application. For more information, refer to *OmniSign – Sign Any Printable Data, Anywhere* in the *DocuSign Signature Appliance Client User Guide*.

The ARX OmniSign printer file name for 64 bit operating systems is ARX OmniSign Printer64.msi.

Installation Pre-requisites

- To perform signatures using Office 2010/2013/2016 upon .docx or .xlsx files, it is mandatory to install .NET Framework version 2 or above on the client machine. The client installation prompts the end user to automatically install .NET framework 2 if it is not already installed. When installing the client on Windows 8, .NET framework 2 must be installed because it is not installed by default.
- To perform signatures upon .docx or .xlsx files using DocuSign Signature Appliance Signature APIs, it is mandatory to install .NET Framework version 3 on the client machine. The installation is not performed automatically by the client installation and should therefore be performed by the user.
- To perform signature field creation upon .docx or .xlsx files using DocuSign Signature Appliance Signature APIs, it is mandatory to install .NET Framework version 3.5 on the client machine. The installation is not performed automatically by the client installation and should therefore be performed by the user.
- To perform signatures upon .xml files using DocuSign Signature Appliance Signature APIs, it is mandatory to install .NET Framework version 2 on the client machine. The installation is not performed automatically by the client installation and should therefore be performed by the user.
- If you intend to use the ARX add-in for Microsoft office, you should include the component called "Visual Basic for applications" when installing Microsoft Office. This component is included in the Microsoft Office installation by default.

Installing the Client Directly from the CD

To install the client directly from the CD:

- Insert the ARX CoSign CD into the CD drive.
- If you are using Windows 7 and above or Win2008R2 and above, you are prompted to select a language. Select the desired language from the list and press **OK**.

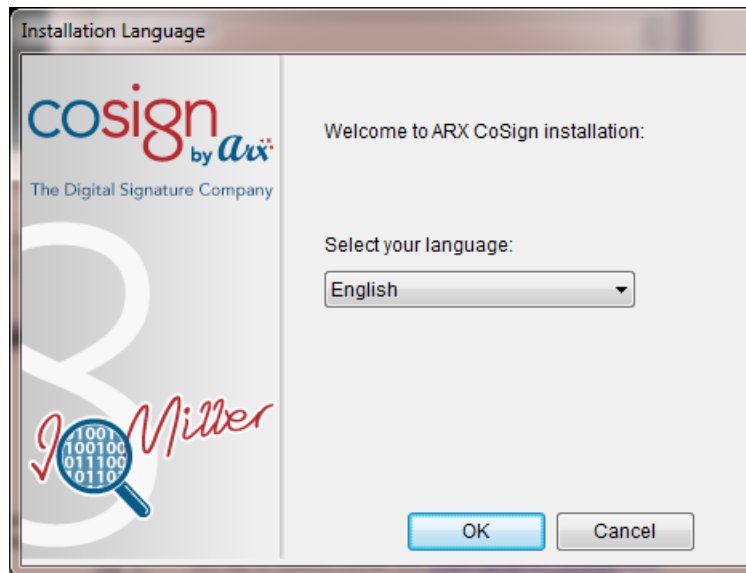


Figure 31 Language Selection Window

The language selection will affect the installation screens, and all end-user Client GUI elements such as OmniSign, the ARX Word Legacy add-in, etc. It will not affect the Configuration Utility or any administrative tools.

The following ARX CoSign Client Installation screen appears:



Figure 32 CoSign Client Components Installation Screen

- Select the components you wish to install, based on the designation of the current workstation. Keep in mind the following:
 - The **ARX CoSign Client** component is always selected.
 - If the workstation is an administrative workstation, select the **ARX CoSign Admin** component.

- If the workstation is a user workstation, select the applicable components: **Microsoft Office**, or **ARX OmniSign Printer**.

Note: The Microsoft Office component is automatically selected if Microsoft Office is installed in the end-user machine.

Note: The OmniSign Printer component installs a new virtual printer in the end-user's machine.

- Click **Install Now**.

When installation is complete, a ✓ appears next to each of the installed components. In case of a failure, an X appears next to the relevant components and a summary information box appears.

Alternatively, you can place the contents of the CD on the network so that end users can install the DocuSign Signature Appliance Client through the network. While this method eliminates the need to use the CD for each installation, it does not facilitate automatic installations of the software.

Automatically Deploying the Client

Refer to [Appendix B: Centralized Client Installation](#) for information on how to automatically deploy the Client on various end user platforms.

Uninstalling the DocuSign Signature Appliance Client

Uninstall the DocuSign Signature Appliance client either locally, or automatically using Microsoft Active Directory.

Uninstalling the DocuSign Signature Appliance Client locally:

To uninstall the DocuSign Signature Appliance client locally:

- Open the **Start** menu and select **Programs** → **ARX CoSign** → **Uninstall CoSign Components**.
- A confirmation box appears. Click **Yes** to uninstall. The uninstalling process begins.
- When the DocuSign Signature Appliance Client is uninstalled from the workstation, a message box appears to inform you that the system finished uninstalling. Click **OK**.

Uninstalling the Client in an Active Directory Environment

Refer to [Appendix B: Centralized Client Installation](#) for information on how to centrally instruct all clients to uninstall their DocuSign Signature Appliance client installation.

Distributing DocuSign Signature Appliance Information through the SCP

The DocuSign Signature Appliance client requires some basic information about the DocuSign Signature Appliance in order to be able to communicate with it. For example, it must know the IP address of the DocuSign Signature Appliance.

When DocuSign Signature Appliance is installed in Microsoft Active Directory, all DocuSign Signature Appliances update a specific location in the directory called *SCP* (Service Connection Point) with the necessary information. The DocuSign Signature Appliance Client automatically updates itself with the necessary information from the SCP.

The following sections provide a description of SCP usage in Microsoft Active Directory.

In an LDAP or Directory Independent environment, you must manually configure each DocuSign Signature Appliance client with the necessary information using the Configuration Utility (refer to [Chapter 8: Configuration Utility](#)). If you wish, you can also use the Configuration Utility to manually configure each DocuSign Signature Appliance client in an Active Directory.

Note: You can use the administrative configuration utility to generate a configuration and distribute it to clients using either a group policy or through other mechanisms such as a login script. For more information, refer to [Appendix B: Centralized Client Installation](#).

Microsoft Active Directory SCP

To view the DocuSign Signature Appliance SCP in a Microsoft Active Directory:

1. In the Administration MMC, navigate to **Active Directory Sites and Services** → **Services** → **NetServices**.

The list of DocuSign Signature Appliances in the network is displayed. Each DocuSign Signature Appliance is listed under the name *DocuSign Signature Appliance Service Connection Point For CSN0001* where CSN0001 is the specific DocuSign Signature Appliance serial number.

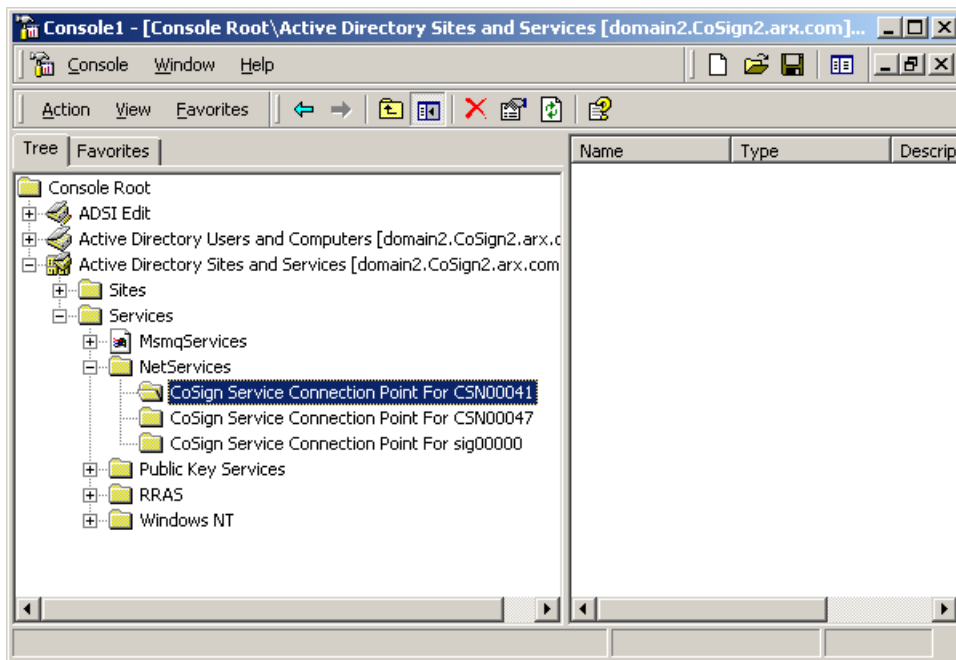


Figure 33 Active Directory SCP

Each entry in the list represents a DocuSign Signature Appliance. The following information is available about each DocuSign Signature Appliance (the information cannot be viewed through the Net Services window):

- ◆ IP address.
- ◆ listening port number.
- ◆ availability status (**Up** or **Down**).

Note: In rare cases where the DocuSign Signature Appliance availability status does not reflect the actual status of the appliance, you can manually set the Up/Down state of a

DocuSign Signature Appliance using the `setscp` utility. Refer to [SetSCP](#) in [Chapter 5: Managing the DocuSign Signature Appliance](#).

- ◆ `prompt for logon` parameter value – Directs the client whether to present a logon popup window for accessing DocuSign Signature Appliance, or whether to use Microsoft mechanisms.
- ◆ `prompt for sign` parameter value – Directs the client whether to display a password window for every signature operation.

The SCP information is updated by each DocuSign Signature Appliance upon installation and upon any modification.

If a DocuSign Signature Appliance is replaced by another appliance or removed from the organizational network, it is recommended to delete the appropriate entry. This ensures that DocuSign Signature Appliance clients will not attempt to connect to irrelevant appliances.

Using the Control Panel

All client-based operations are activated through the Control Panel.



Figure 34 CoSign Control Panel

Some Control Panel options are always active, while others are active depending on the status of the DocuSign Signature Appliance (Installed/Not Installed) or the type of DocuSign Signature Appliance installation (Microsoft Active Directory, LDAP, or Directory Independent).

The following sections describe the actions available from the Control Panel:

User Actions

Client Configuration – This option enables the end user to configure the DocuSign Signature Appliance client settings. Refer to [Chapter 8: Configuration Utility](#) for more information.

Graphical Signatures – This option enables both end users and administrators to manage personal graphical signatures. For more information, refer to [Using the Graphical Signature Management Application](#).

Change Password – This option is relevant only in the case of a Directory Independent environment. For more information, refer to [Directory Independent Environment Options](#).

This option includes also the User Activation operation that is mandatory when DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.

OmniSign Settings – This option activates the OmniSign application in configuration mode. In this mode the user can setup the appearance and other parameters related to the digital signature created using OmniSign. For more information related to OmniSign, refer to OmniSign – Sign Any Printable Data, Anywhere in the DocuSign Signature Appliance Client User Guide.

Logoff – This option logs off from the session. This option is relevant when DocuSign Signature Appliance is installed in a Directory Independent environment, or any other configuration where the user needs to login manually.

Administrator Actions

Note: The Administrator Actions are relevant only if the administrative client is installed.

Appliances Management – This option displays the Administration MMC. Using the Administration MMC it is possible to install or restore the appliance, or manage it in operation mode. Refer to [Chapter 3: Installing DocuSign Signature Appliance](#) and [Chapter 5: Managing the DocuSign Signature Appliance](#) for more information related to the Administration MMC.

Users Management – This option activates the Users Management application. This application is mandatory when DocuSign Signature Appliance is installed in a Directory Independent environment, but can also help the administrator to view users' statuses in all other installation environments.

Client Configuration Management – This option activates the Configuration Utility in administrative mode. For more information, refer to [Chapter 8: Configuration Utility](#).

CoSign Control Panel Menu Bar

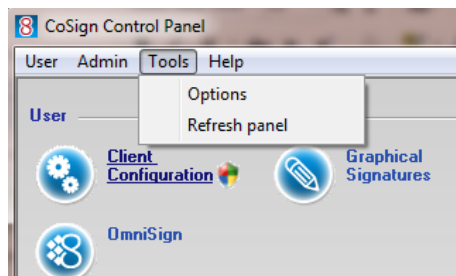


Figure 35 CoSign Control Panel Menu Bar

The **User** and **Admin** options of the Control Panel menu bar display all the options that can be activated from the Control Panel.

In addition, the Tools option includes two options.

- **Options** – This enables you to configure Control Panel settings. When you select **Options** from the **Tools** menu, the following dialog box appears:

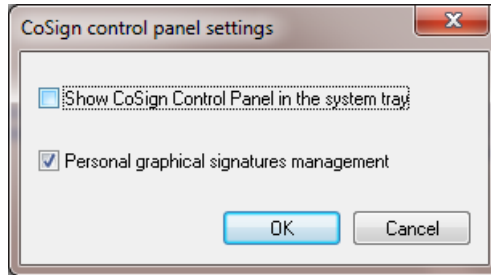


Figure 36 CoSign Control Panel Settings

- **Show Control Panel in system tray** – Check this option to display the Control panel in the system tray when the Control Panel is activated.
- **Personal graphical signature management** – Check this option to activate the graphical signature application in user mode. If the option is unchecked and the administrative client is installed, the graphical signature application will operate in administrative mode. Refer to [Using the Graphical Signature Management Application](#).
- **Refresh Panel** – This option updates the icons in the control panel according to the updated state of the DocuSign Signature Appliance.

Control Panel – Tray Item

The control panel icon appears in the tray if the option **Show CoSign Control Panel in system tray** is selected. Right-click the icon to display a popup that enables you to perform the following operations:

- **Open control panel** – Maximizes the control panel.
- **Change password** – Relevant only for a Directory Independent environment. Refer to [Directory Independent Environment Options](#). This operation includes also the User Activation operation that is mandatory when DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.
- **Logoff** – Refer to the description of Logoff in [User Actions](#).
- **Exit** – Closes the control panel.

Directory Independent Environment Options

The following options are relevant only for a Directory Independent environment.



Figure 37 CoSign Control Panel – Directory Independent Environment

Changing the Password

To change your password when DocuSign Signature Appliance is installed in a Directory Independent environment:

1. Click **Change User Password** in the Control Panel (Figure 37).

The *Change Password* window appears.

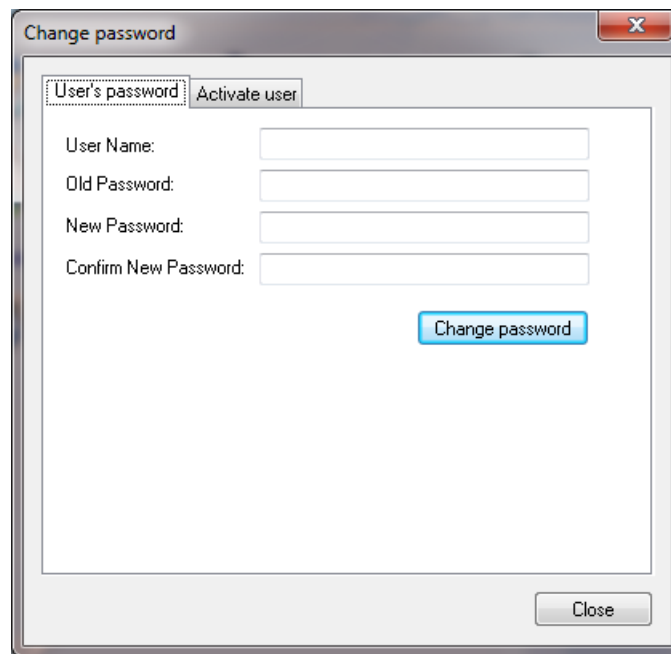


Figure 38 Change Password in a Directory Independent Environment

2. Enter your user name.
3. Enter the old password of the account and the new password of the account. Confirm the new password.
4. Click **Change password**.

Performing User Activation

To activate your account when DocuSign Signature Appliance is installed in a Common Criteria EAL4+ environment:

1. Click **Change User Password** in the Control Panel (Figure 37).
The Change Password window appears (Figure 38).
2. Select the **User's activation** tab.

The screenshot shows a 'Change password' dialog box with two tabs: 'User's password' and 'User's activation'. The 'User's activation' tab is selected. It contains five text input fields: 'User Name:', 'Old Password:', 'New Password:', 'Confirm New Password:', and 'OTP Password:'. Below these fields is an 'Activate User' button. At the bottom right of the dialog is a 'Close' button.

Figure 37 User Activation Window

3. Enter your user name.
4. In the **Old Password** field enter the Activation password of the account.
5. In the **New Password** and **Confirm New Password** fields enter a new password of your choice. The password must follow organizational password policy rules.
6. Enter an OTP as it appears in your personal OTP device.
7. Click **Activate User**.

The user account is now activated. You can start working with DocuSign Signature Appliance – perform key and certificate enrollment, upload graphical images, and sign using your key.

Note: Activation can be performed only once per account.

Note: If you get a message that the account was already activated, this may indicate a security breach.

Using the Graphical Signature Management Application

The Graphical Signature Management application enables you to view all your graphical signatures and create a new graphical signature. This graphical signature can be attached to all Microsoft Word, Excel, InfoPath, Tiff, and Adobe Acrobat documents that you sign.

The Graphical Signature application is automatically installed together with the ARX DocuSign Signature Appliance Client component.

The Signature application can be used in either of two modes of operation:

- **Administrative Mode** – An administrator station is used for creating the user’s graphical signatures, as follows: The user supplies his/her identity and password, after which the user can create and then view his/her own graphical signatures.
- **User Mode** – The user can create or view his/her own graphical signatures.

There are several mechanisms that can be used for capturing a graphical signature:

- A capturing device such as Topaz pads or Interlink pads.
- A mouse or a tablet PC.
- A text-based graphical signature.
- An image uploaded from a file.

The following section details how to capture graphical signatures.

If you do not capture a graphical signature, a default graphical signature that is based on your name is used by the signing application, such as Office 2010/2013/2016 or OmniSign.

Installing the Graphical Signature Capture Device

The DocuSign Signature Appliance appliance is supplied with a graphical signature capture device. However, you can use any of the following types of graphical signature capture devices:

- Graphical signature capture devices produced by Topaz Systems (<http://www.topazsystems.com>). Two models are available:
 - SigLite LCD 1x5 USB – This model includes an LCD capture device. The entered graphical signature appears on the LCD screen.
 - SigLite 1x5 USB – This model does not include an LCD capture device.



Figure 39 SigLite LCD 1x5 USB

- Graphical signature capture devices produced by Interlink Electronics (<http://www.interlinkelectronics.com>). Two models are available:
 - ePad-ink – This model includes an LCD capture device. The entered graphical signature appears on the LCD screen.
 - ePad – This model does not include an LCD capture device.



Figure 40 ePad-ink



Figure 41 ePad

Note: Install the signature capture device only on machines in which the administrative client is installed.

To install the graphical signature capture device:


- Connect the signature capture pad to the USB port on the workstation. The pad's drivers are automatically installed.

Managing Graphical Signatures

The Graphical Signature Management application enables you to create and manage graphical signatures. The graphical signatures you create using this utility are stored inside the DocuSign Signature Appliance's users database as graphical objects.

This section describes how to operate the Graphical Signature Management application in Administrative mode, in which different users typically use the administrator machine to create their graphical signatures. Certain options that are relevant only to User mode are not described here, but rather in the *DocuSign Signature Appliance Client User Guide*.

To manage your graphical signatures:

- Open the **Start** menu and select **Programs**→ **ARX CoSign**→ **CoSign Control Panel**, or you can double-click the CoSign icon  in the tray. The Control Panel appears.
- If the signature application is operating in user mode and you would like it to operate in administrative mode, perform the following:
 - Select **Options** from the **Tools** menu in the Control Panel. The Control Panel Settings window appears ([Figure 36](#)).
 - Make sure that the **Personal graphical signature management** option is not selected.
- In the Control Panel, click **Graphical Signature**. An empty Graphical Signatures Viewer dialog box appears.

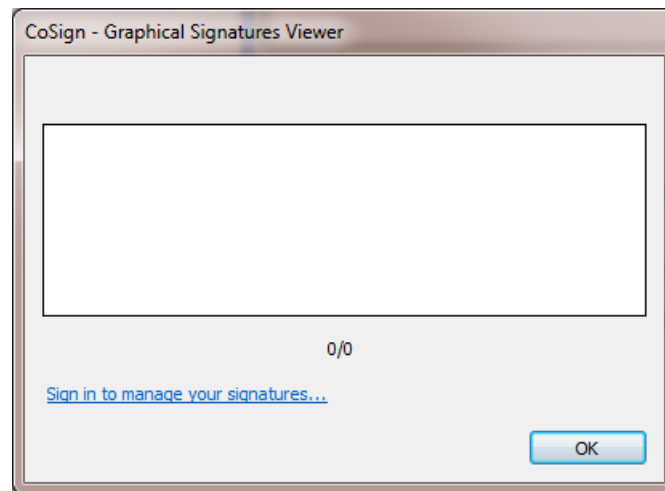


Figure 42 Empty Graphical Signatures Viewer Dialog Box

- Click **Sign in to manage your signatures**. A window appears for entering your login information (similar to Figure 43).

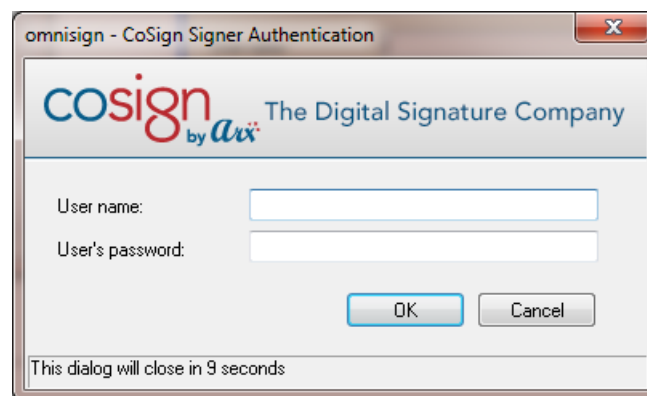


Figure 43 Enter Login Information Dialog Box

- Enter your login information and click OK.
The *ARX Graphical Signature Viewer* dialog box appears, for managing your graphical signatures.

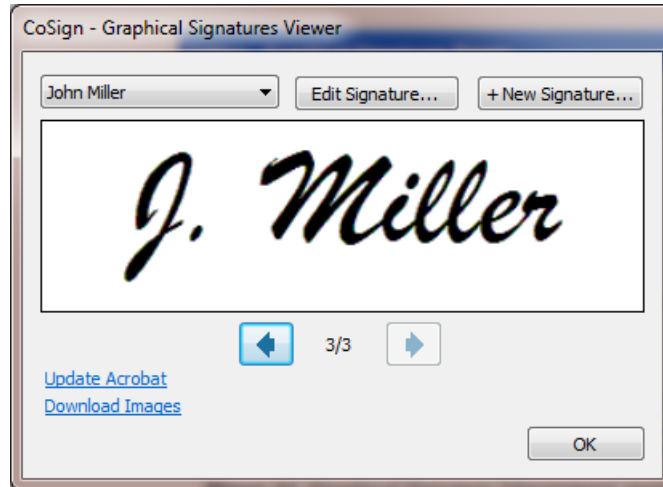


Figure 44 Graphical Signature Management Application

- Select a signature from the drop down list at the top of the window. The corresponding graphical image appears in the middle of the window.

You can also use the left and right arrows to browse through all the available graphical signatures – those stored in the DocuSign Signature Appliance, and also those located in the local *wetInk*, *Logo*, or *Initials* folders, under *My Documents/My Pictures/My CoSign images*.

Note: The **Update Acrobat** and **Download Images** options are relevant only in User mode. For information, refer to the *DocuSign Signature Appliance User Guide*.

- If you click either **New Signature** or **Edit Signature**, the *New Signature* or *Edit Signature* dialog box appears.

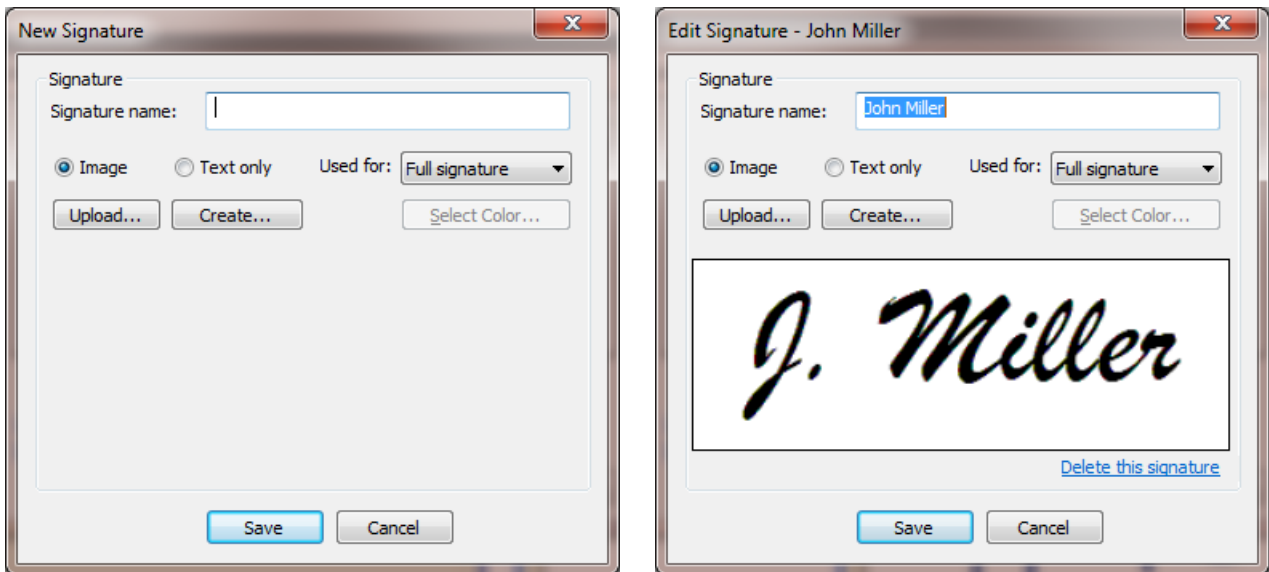


Figure 45 New Signature and Edit Signature Dialog Boxes

The display area displays the currently selected graphical signature.

The following options are available:

- **Signature Name** – Specify the name of the edited graphical signature.
- **Image/Text Only** – Specify if the loaded graphical signature is based on an image or text. Depending on the selected option, the set of actions is different. Refer to [Creating an Image-Based Graphical Signature](#) and [Creating a Text-Based Graphical Signature](#).
- **Used For** – Specify the type of graphical signature: Full Signature, Initials, or Logo. A single logo is allowed per user.
- **Select Color** – Specify the color of the foreground of the image. This is available for monochrome images.
- **Delete this signature** – Available in the *Edit Signature* dialog box only. The currently selected graphical signature is deleted.

Note: A graphical signature is limited to 29KB. You can use up to a maximum of 140KB for your entire set of graphical signatures. If you wish to use a larger graphical image, you can store it in a local directory as described at the beginning of this section. Each local graphical signature is limited to 1 MB.

Note: The first time you create a signature using a signature capture device, you must have local administrative rights. Afterwards, any user can create a signature.

Creating an Image-Based Graphical Signature

If you select **Image** in the *Edit Signature* dialog box (Figure 45), you can create an image-based graphical signature in any of the following ways:

- Upload any local image file to DocuSign Signature Appliance. Refer to [Uploading an Image File](#).
- Create an image file and load it into DocuSign Signature Appliance. Refer to [Creating an Image File](#).

Uploading an Image File

To load an image file into DocuSign Signature Appliance:

- Select **Image** in the *Edit Signature* dialog box (Figure 45).
- Click **Upload**.
- In the browse window that appears, browse to the desired image file. You can upload the following types of graphic files: monochrome bmp, multicolor bmp, or jpg.

If the size of the image is larger than the maximal size allowed, it is automatically reduced. A window appears (Figure 46), asking whether to upload the reduced size image to the DocuSign Signature Appliance.

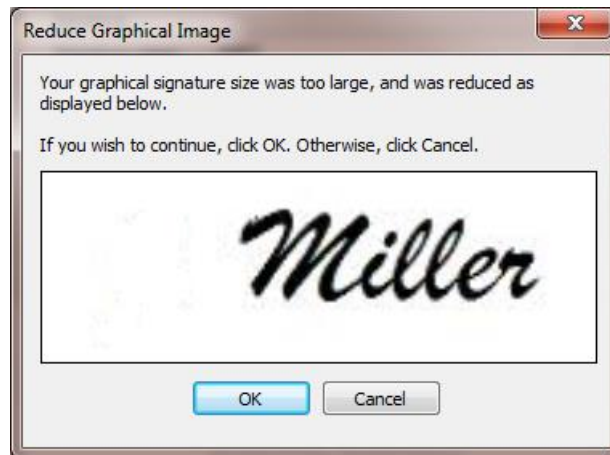


Figure 46 Reduce Graphical Image Dialog Box

Creating an Image File

To create an image file and upload it to DocuSign Signature Appliance:

- Select **Image** in the *Edit Signature* dialog box (Figure 45).
- Click **Create**. A list of available image capturing techniques appears.

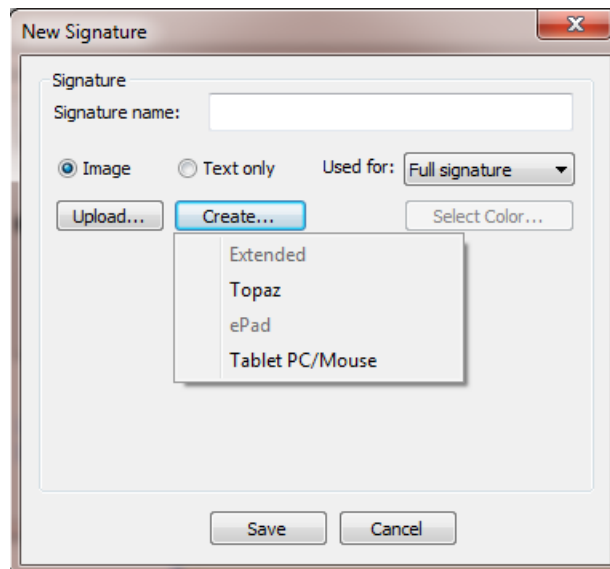


Figure 47 Create a Graphical Signature – List of Image Capturing Techniques

Select an image capturing technique while keeping the following in mind:

- **Topaz or ePad** – Use these options when it is required to enter the graphical signature using a signature capture pad. Use the pad as described in [Installing the Graphical Signature Capture Device](#). If you are using a signature capture device with no LCD display, you will be able to see the signature only on the PC screen while editing it. If you are using a signature capture device with an LCD display, you will be able to see the signature both on the device and on the PC screen while editing it.

- **Tablet PC/Mouse** – Use a Tablet PC and a pen or a regular PC mouse to enter a new graphical signature. Any movement of the mouse or pen in the tablet PC is drawn in the *Capture Signature* window that appears.

Note: You will be able to use the mouse on a regular PC only when using Window 7 and above or when Microsoft Office 2010/2013/2016 is installed.

The display in the *Edit Signature* window refreshes (see Figure 48).

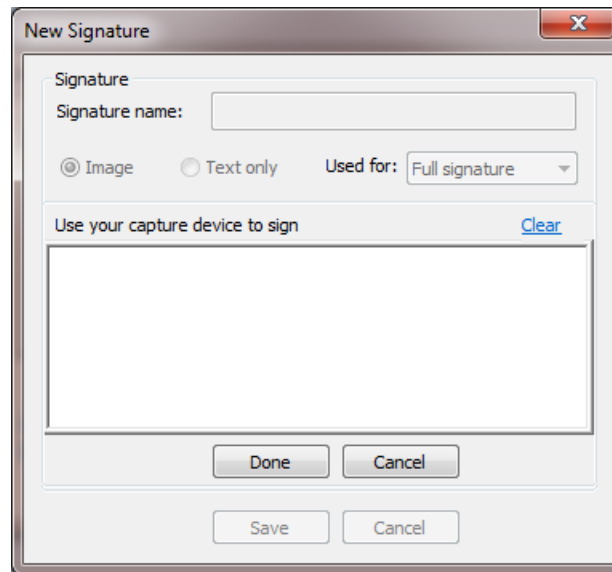


Figure 48 Creating a Graphical Image File

- Use the capturing technique to capture a graphical signature.
- When capturing is complete, click **Done** in the *Edit Signature* dialog box (Figure 48). The graphical signature you created is uploaded into DocuSign Signature Appliance.
- If you wish to re-start the capture, click **Clear**.

Note: If the size of the image is larger than the maximal size allowed, the image size is automatically reduced.

Creating a Text-Based Graphical Signature

To create a text-based graphical image:

- Select **Text only** in the *Edit Signature* dialog box (Figure 45). The options shown in Figure 49 appear.



Figure 49 Edit Signature Dialog Box– Text-based Graphical Signature

- Click **Font**. A *Font* dialog box appears.

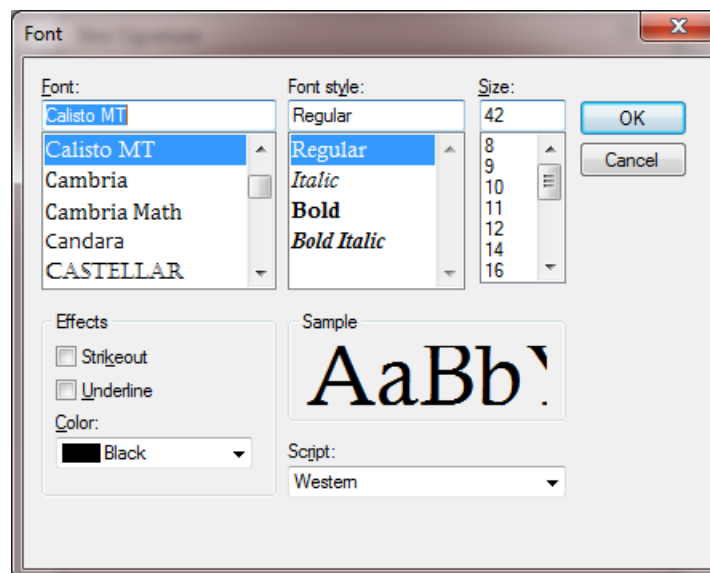


Figure 50 Edit Signature Dialog Box– Text-based Graphical Signature – Defining the Text Appearance

- In the *Font* dialog box, specify the appearance of the graphical signature text (font, size, color, etc.).
- Click **OK** to close the *Font* dialog box.
- Using your keyboard, enter the text for the graphical signature. The signature is displayed, with the appearance you defined, in the window of the *Edit Signature* dialog box (Figure 49).

Installing the Root Certificate and CoSign Verifier

In order to sign or validate documents originating from an organization, you must install on your workstation the organization's ROOT certificate. In addition, if you do not have a Client, you need to install a CoSign Verifier in order to validate signatures of Office XP/2003 documents and Adobe documents.

For a full explanation of how to install a ROOT certificate and a CoSign Verifier, refer to the section *Installing the Root Certificate and CoSign Verifier* in the *DocuSign Signature Appliance User Guide*.

Adding the ROOT Certificate to a Trusted CA List (Active Directory only)

It is possible to add the ROOT certificate to a trusted CA list in the Active Directory of the domain. Every workstation connected to the domain automatically obtains the ROOT certificate and places the certificate in its local trusted ROOT CA list.

To add the ROOT certificate to a trusted CA list, use the Microsoft utility `certutil.exe`. The utility is part of Windows Server 2003 and Windows Server 2008. It is also available as part of the Microsoft Windows Server 2003 Administration Tools Pack which can be downloaded from <http://support.microsoft.com>.

Execute `certutil.exe` as follows:

```
certutil.exe -dspublish -f <file name> RootCA
```

where:

-f forces the creation of the object if it doesn't exist, and
<file name> is the certificate file name.

Note: The user who runs `certutil.exe` needs permissions for creating an object under `Services\public key services\Certificate authorities` and under `Services\public key services\AIA`.

Using CoSign Verifier for Validation Purposes

To validate a document, you need to install the root certificate of the organization that signed the document. You do not need a DocuSign Signature Appliance Client or DocuSign Signature Appliance. However, if you do not have a DocuSign Signature Appliance Client, you need to install a CoSign Verifier if you wish to validate signatures of Office XP/2003 documents and Adobe documents.

For a full explanation of how to install a ROOT certificate and a CoSign Verifier, refer to the section *Installing the Root Certificate and CoSign Verifier* in the *DocuSign Signature Appliance User Guide*.

- For more information on verifying Office XP/2003 documents, refer to Signing Microsoft Office Documents in the DocuSign Signature Appliance User Guide.
- For more information on verifying Adobe documents, refer to Signing Adobe Acrobat Documents in the DocuSign Signature Appliance User Guide.

Extended Authentication Modes

DocuSign Signature Appliance enables the use of extended authentication modes, in addition to the regular authentication mode which is based on a User ID and password authentication.

The extended authentication mode is required in more sensitive user environments, where the digital signature process requires the end user to prove his/her identity based on additional devices such as OTP

(One Time Password) devices, SmartCard for authentication, or a Biometric device. Depending on the configured Extended Authentication, the end user is prompted during the digital signature operation to supply information according to the Extended Authentication mode used.

The following Extended Authentication modes are supported:

- *OTP based on Radius authentication* – The end user is prompted to provide the OTP during the digital signature operation.
The DocuSign Signature Appliance interfaces with the OTP server using a Radius protocol. The Radius protocol enables the DocuSign Signature Appliance to interact with the OTP server and send the user ID and the OTP in a secret manner.
The OTP is sent as is to the RADIUS server. There are some RADIUS servers whose password is based both on static and dynamic passwords. In these cases, both the static and dynamic password are passed to the RADIUS server for authentication.
If the user is approved by the OTP server, DocuSign Signature Appliance continues to perform the digital signature operation.
For more information about the various parameters that require configuration in order to interface to the RADIUS server, refer to [Extended Authentication](#).
Note: DocuSign Signature Appliance supports a maximum password length of 128 characters.
If DocuSign Signature Appliance is operating in Common Criteria EAL4+ mode, OTP is used for every digital signature operation. In addition, because the OTP must be validated within the DocuSign Signature Appliance, initial additional integration is required within the Radius Server for interacting with the DocuSign Signature Appliance for the purpose of OTP validation. For information, contact ARX.
- *Authentication SmartCard* – The end user enters the authentication SmartCard in a dedicated smart card reader device.
The user is prompted for a PIN to access the SmartCard, and the SmartCard is used to prove the user identity to the DocuSign Signature Appliance.
The DocuSign Signature Appliance authenticates the user, and if the user is approved, DocuSign Signature Appliance continues to perform the digital signature operation.
This solution requires a special component in the DocuSign Signature Appliance Client. For more information, contact ARX support at <http://www.arx.com/support/supportrequest>.
- *Biometric Device* – The end user uses a biometric device. A proof of identity is sent to the DocuSign Signature Appliance as part of the digital signature operation.
The DocuSign Signature Appliance checks the identity of the user, and if approved, DocuSign Signature Appliance continues to perform the digital signature operation.
This solution requires a special component in the DocuSign Signature Appliance Client. For more information, contact ARX support at <http://www.arx.com/support/supportrequest>.
To configure DocuSign Signature Appliance to use extended authentication, refer to [Extended Authentication](#).

Chapter 5: Managing the DocuSign Signature Appliance

The DocuSign Signature Appliance is managed via the Administration Microsoft Management Console (MMC). This chapter describes how to use the Administration MMC for the most efficient DocuSign Signature Appliance management.

This chapter also describes ARX's *Users Management* GUI utility, which provides easy users' management for cases where DocuSign Signature Appliance is installed in a Directory Independent environment or other environments. It is also possible to manage users in this environment through a DocuSign Signature Appliance API (Application Programming Interface) called Signature Local User Management API. DocuSign Signature Appliance Signature APIs documentation is located in the `SAPI\doc` folder of the SDK CD.

Note: Managing DocuSign Signature Appliance differs slightly depending on whether it is installed in a Microsoft Active Directory, LDAP, or Directory Independent environment. These differences are mentioned throughout the chapter.

Prerequisites to Using the Administration MMC

The Administration MMC enables you to efficiently manage the DocuSign Signature Appliance. In order to use the Administration MMC, you must have the following qualifications:

- You must be the built-in administrator defined during DocuSign Signature Appliance installation;
- Or
- You must belong to the domain's administrative group as well as a valid DocuSign Signature Appliance user. For example, in a typical Active Directory installation, you must belong to the DocuSign Signature Appliance Signers group. The administrative group is defined by the system parameter *Administrator Group*, as described in [Users Directory Parameters](#). In the case of a Directory Independent environment, you must be defined with DocuSign Signature Appliance Admin appliance management rights.
- Before performing any appliance administrative activity, you must manually login to DocuSign Signature Appliance using either the built-in administrator or another valid administrator account.

Starting the Administration MMC

To start the Administration MMC:

- Open the **Start** menu and select **Programs** → **ARX CoSign** → **CoSign Control Panel**.
- Select **Appliances Management**.

The ARX CoSign Appliance Management window appears, showing all installed DocuSign Signature Appliance appliances ([Figure 51](#)).

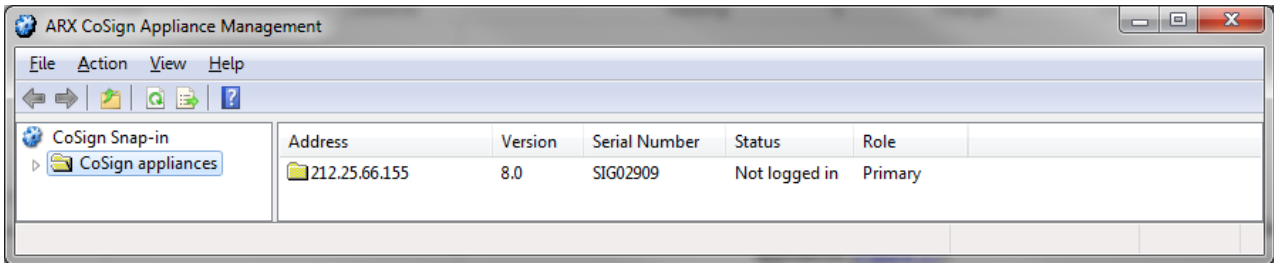


Figure 51 ARX CoSign Appliance Management Window

- Right-click the DocuSign Signature Appliance you wish to administrate.
- From the popup menu, login to DocuSign Signature Appliance as an appliance administrator by selecting **All Tasks** → **Login** → **Login**, or **All Tasks** → **Login** → **Login built-in user**.

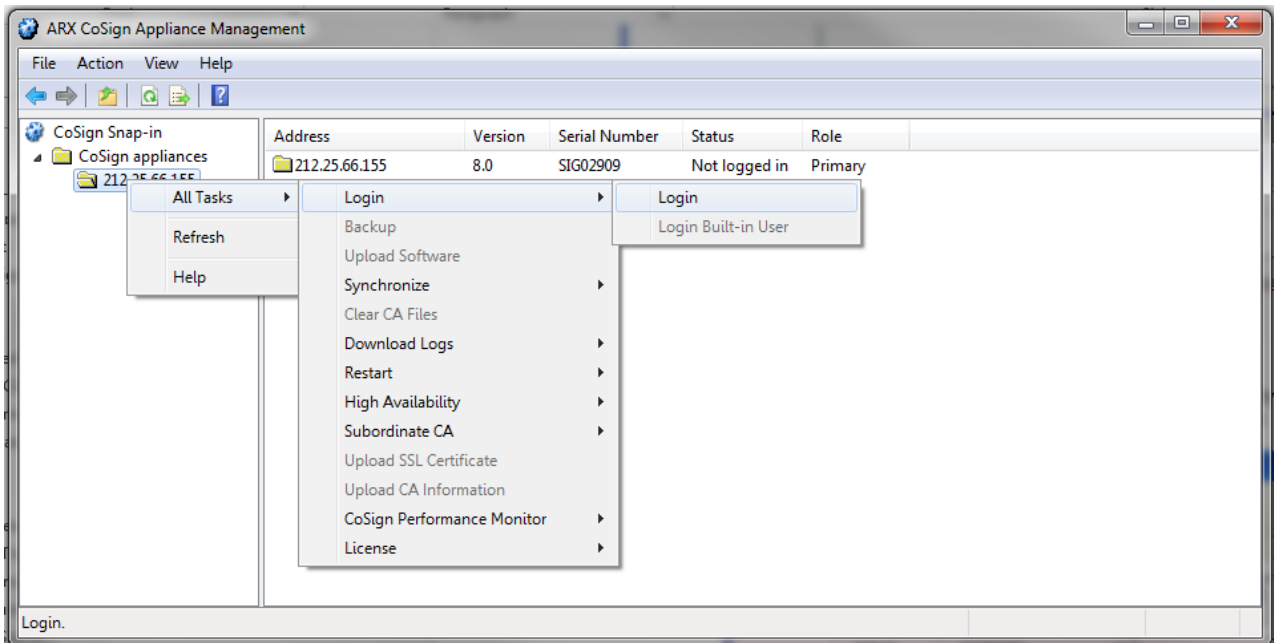


Figure 52 ARX CoSign Appliance Management Window – Logging in to CoSign as an Appliance Administrator

Note that in the regular login option you can use your Active Directory / LDAP / Directory Independent admin user for connecting to DocuSign Signature Appliance. If you choose to use the built-in user login, you must provide the account name and password.

Administration MMC Capabilities

Once you are logged in to the Administration MMC, you can perform the following operations, described in detail below:

- Back up the current DocuSign Signature Appliance data.
- Upload software updates provided by ARX.
- Manually synchronize DocuSign Signature Appliance with your Microsoft Active Directory or LDAP directory.

- Synchronize DocuSign Signature Appliance with the External CA. This option is relevant when DocuSign Signature Appliance is interfacing with an external CA automatically for producing users' certificates.
- Refresh Certificates.
- Clear CA files. This option is relevant when DocuSign Signature Appliance is using an internal CA for producing certificates. This option clears internal CA information. This option is not relevant for CoSign 4.4 and above.
- Download log files from the DocuSign Signature Appliance.
- Restart or shut down DocuSign Signature Appliance.
- Configure high availability options.
- Manage the Subordinate CA Certificate. This option is used when installing or renewing a subordinate CA certificate.
- Upload a new SSL Server certificate to be used as part of the Web Services offering. This operation is also relevant if the Web Services interface that is based on Rest API is used.
- Extract technical performance figures on the internal activity of the appliance.
- Prepare a request for a new DocuSign Signature Appliance license and upload the new license.
- View and modify system parameters.
- Restore the DocuSign Signature Appliance from backup data.
- Install a new DocuSign Signature Appliance (refer to [Installing the Appliance Software](#)).
- Install an alternate DocuSign Signature Appliance (refer to [Installing an Alternate DocuSign Signature Appliance](#)).

Backing up the DocuSign Signature Appliance Data

You can back up the entire DocuSign Signature Appliance database (which includes all the users' keys, certificates, and graphical signatures), the internal CA files, and all the DocuSign Signature Appliance configuration data, to a file located on your local network. The generated backup file is encrypted and can only be decrypted by the DocuSign Signature Appliance. The DocuSign Signature Appliance key is generated and stored on the backup MiniKey token during appliance installation.

After generating the backup file, you can save it to a disk or CD to store in case of data loss. This file can then be used to restore the DocuSign Signature Appliance if necessary. For more information on restoring the DocuSign Signature Appliance, refer to [Restoring the Appliance](#).

To back up the DocuSign Signature Appliance database:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the appliance you wish to back up.
- From the popup menu, select **All Tasks** → **Backup**. The *Select a File* dialog box appears.
- Select a local backup file and click **Save**. The DocuSign Signature Appliance backup in progress status bar appears. When the backup operation is complete, the following message appears:
Backup finished successfully.

Very Important: After any upgrade, you must perform a backup of the appliance.

Very Important: You must perform a backup procedure periodically to enable quick recovery in the case that important information, such as users' graphical signatures, is removed from the DocuSign Signature Appliance, or in the case of any appliance hardware problem.

Note: You can also perform backup using the command line utility `GetBackup` (refer to [Using Command Line Utilities](#)).

Upgrading

You can upload software updates provided by DocuSign. The software updates are signed by DocuSign to ensure security. Software updates can be either a major version upgrade or a software patch. The same procedure is used in both cases.

Before uploading an upgrade or a patch, use the Console's **Status** menu to verify the existing appliance software version (refer to [Displaying Status](#)).

Note the following:

- If you wish to upgrade from version 6.0, or 6.3, you must first upgrade to version 7.1, then upgrade to version 7.4, upgrade to version 7.5 and finally upgrade to version 8.0.
- If you wish to upgrade from version 7.1, you must first upgrade to version 7.4, then upgrade to version 7.5 and finally upgrade to version 8.0.

Note: For information on how to upgrade DocuSign Signature Appliances in a high availability environment, refer to [Upgrading Appliances Participating in a High Availability Cluster](#).

Very Important: After any upgrade, you must perform a backup of the appliance.

Note: If DocuSign Signature Appliance is deployed in Common Criteria EAL4+ mode, you can only upgrade the DocuSign Signature Appliance to new versions that are Common Criteria certified.

Upgrading to Version 7.1

CoSign version 7.1 includes a software upgrade from CoSign version 6 or 6.3 to version 7.1. The upgrade consists of the following file: `verupd71.dlm`.

To upgrade from version 6/6.3 to version 7.1:

- Load `verupd71.dlm` from the CoSign version 7.1 CD.
- Follow the instructions listed in [Uploading a Software Update](#). The upgrade runs immediately.
- Use the Console's **Status** menu to verify that the software version is `SW7.1`. (refer to [Displaying Status](#)).

Upgrading to Version 7.4

CoSign version 7.4 includes a software upgrade from CoSign version 7.1 to version 7.4. The upgrade consists of the following file: `verupd74.dlm`.

To upgrade from version 7.1 to version 7.4:

- Load `verupd74.dlm` from the CoSign version 7.4 CD.
- Follow the instructions listed in [Uploading a Software Update](#). The upgrade runs immediately.
- Use the Console's **Status** menu to verify that the software version is `SW7.4`. (refer to [Displaying Status](#)).

Upgrading to Version 7.5

CoSign version 7.5 includes a software upgrade from CoSign version 7.4 to version 7.5. The upgrade consists of the following file: `verupd75.dlm`.

To upgrade from version 7.4 to version 7.5:

- Load `verupd75.dlm` from the CoSign version 7.5 CD.
- Follow the instructions listed in [Uploading a Software Update](#). The upgrade runs immediately.
- Use the Console's **Status** menu to verify that the software version is `SW7.5`. (refer to [Displaying Status](#)).

Upgrading to Version 8.0

DocuSign Signature Appliance version 8.0 includes a software upgrade from CoSign version 7.5 to version 8.0. The upgrade consists of the following file: `verupd80.dlm`.

To upgrade from version 7.5 to version 8.0:

- Load `verupd80.dlm` from the version 8.0 CD.
- Follow the instructions listed in [Uploading a Software Update](#). The upgrade runs immediately.
- Use the Console's **Status** menu to verify that the software version is `SW8.0`. (refer to [Displaying Status](#)).

Uploading a Software Update

To upload a software update:

- In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the DocuSign Signature Appliance to which you wish to upload the software.
- From the popup menu, select **All Tasks** → **Upload Software**. The *Select a File* dialog box appears.
- Select a local software update file and click **Open**. The Uploading Software in progress status bar appears. When the upload operation is complete, the following message appears:

Software uploaded successfully.

Note: Since most of the upload operation is carried out after the success message is displayed, it is recommended to view the new version number in the DocuSign Signature Appliance's console or view the log files to validate the success of the operation.

Synchronizing DocuSign Signature Appliance with the Directory Service

Note: This option is not relevant in a Directory Independent environment.

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

DocuSign Signature Appliance monitors and retrieves information directly from the directory service.

During DocuSign Signature Appliance installation, the DocuSign Signature Appliance users are defined either by defining a ROOT OU of all the signers or by defining a signers group (relevant only to Active Directory installations). When a user is added to the directory service and is classified as a signer, DocuSign Signature Appliance automatically generates a key and a certificate for the user, depending on the certificate model used. When a user is deleted from the directory service, DocuSign Signature Appliance automatically removes the user and the user's key and certificate from the DocuSign Signature Appliance. When a user's information is updated in the directory service (e.g., the user's email address is modified), DocuSign Signature Appliance automatically generates a new certificate for the user. In this way, DocuSign Signature Appliance and the directory service remain synchronized.

In certain cases, however, DocuSign Signature Appliance may lose synchronization with the directory service. This may occur if you run DocuSign Signature Appliance with a license for fewer users than necessary, or if the directory service is restored from an old backup. Once the license issue is resolved or the restore operation complete, you can use the **Sync with the Directory** option to manually trigger synchronization of DocuSign Signature Appliance with the directory service.

Another case requiring manual synchronization of the directory is the case where an Active Directory environment is used, and DocuSign Signature Appliance users are based on a dedicated Signers group defined in the Active Directory. When users are removed from the Signers group in the Active Directory, they are not automatically deleted from DocuSign Signature Appliance to prevent users losing their keys and graphical signatures in cases where users are removed and immediately entered back into the Signers group. These users will not be able to sign using DocuSign Signature Appliance, but if it is required to remove these users from DocuSign Signature Appliance, it is necessary to perform the manual synchronization operation.

Note: DocuSign Signature Appliance may lose synchronization also if you modify the DocuSign Signature Appliance OU (Organizational Unit) in the Active Directory environment. Keep in mind that performing a synchronization operation after renaming the DocuSign Signature Appliance OU may cause deletion of all the users in the DocuSign Signature Appliance, including deleting their key, certificates, and graphical signatures. ARX therefore recommends not modifying the DocuSign Signature Appliance users OU after installation.

Note: If DocuSign Signature Appliance is installed in an LDAP or AD Multiple Domains environment, full synchronization is automatically performed periodically. The frequency of synchronization depends on a system parameter (refer to [Changing System Parameters](#)).

Note: In the case of LDAP or AD Multiple Domains installations, running Directory synchronization only updates users information in DocuSign Signature Appliance or deletes users from DocuSign Signature Appliance. Any addition of new users to DocuSign Signature Appliance requires the user to access the DocuSign Signature Appliance.

The **Sync with the Directory** option compares DocuSign Signature Appliance users to directory service users, adding and deleting DocuSign Signature Appliance users, keys, and certificates where necessary.

To manually trigger synchronization of DocuSign Signature Appliance with the directory service:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the desired DocuSign Signature Appliance.
- From the popup menu, select **All Tasks** → **Synchronize** → **Sync with the Directory**. The following message appears:

Do you really want to sync with the Directory?

- Click **OK** to confirm the operation. When the synchronization operation begins, the message **Sync with the Directory started** appears.

Note: The synchronization operation may take a long time. This message only indicates that the operation started. A message in the Event log indicates when the operation is complete.

Synchronizing DocuSign Signature Appliance with the External CA in Automated mode

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

If you are using an external CA in automated mode, you can synchronize the DocuSign Signature Appliance database and the external CA.

This option can be used when interfacing with the Comodo CA.

Use this option when there are valid DocuSign Signature Appliance users who are in the process of receiving an external CA certificate, but have not yet received the certificate.

To synchronize DocuSign Signature Appliance with the external CA:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the DocuSign Signature Appliance you wish to synchronize.
- From the popup menu, select **All Tasks** → **Synchronize** → **Sync with the CA**.

Synchronization includes the following:

- Every certificate in the external CA that does not have a matching user in DocuSign Signature Appliance, is revoked.
- For every user in DocuSign Signature Appliance who does not have a certificate in the external CA, a new certificate request is issued to the CA, and the resultant certificate is sent to DocuSign Signature Appliance.

Note: Users that no longer exist in DocuSign Signature Appliance do not appear in Comodo's CRL, because some applications fail to validate signatures for revoked users who signed the document

when their certificate was valid. If the CRL were to include users that no longer exist in DocuSign Signature Appliance, their valid signatures might appear as invalid.

Refreshing Certificates

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in Common Criteria EAL4+ mode of operation.

This option instructs the DocuSign Signature Appliance to generate new certificates for all the signers. This option should be used in cases where a certain parameter that affects the content of the certificate has changed (for example, the CRL Distribution point of the certificate), and you want to generate new certificates containing the new value for all end-users.

This option can be used also when an automated external CA is configured.

To refresh all users' certificates:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the DocuSign Signature Appliance.
- From the popup menu, select **All Tasks** → **Synchronize** → **Full User Certificate refresh**.
- Confirm the operation.

Following synchronization:

- A new certificate is generated for every end-user, based on the current parameters.
- If DocuSign Signature Appliance interfaces an external CA in automated mode, a certificate renewal procedure is run for every end user.

Note: The Refresh Certificates option is relevant also when DocuSign Signature Appliance interfaces an external CA automatically. Keep in mind that this option will generate new certificates for all users.

Clearing CA files

This option reduces the size of the files used by the internal CA. This subsequently reduces the size of a backup operation.

Note: This option is not relevant to CoSign 4.5 and above.

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in Common Criteria EAL4+ mode of operation.

To clear the CA files:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the desired DocuSign Signature Appliance appliance.
- From the popup menu, select **All Tasks** → **Clear CA Files**.

At the end of the operation a success or failure message appears.

Downloading Log Files

There are three types of DocuSign Signature Appliance log files that you can download:

- **Appliance Event log** – Displays signing operations, major errors, and administrative actions, such as performing backups.
- **Appliance Debug log** – Displays internal debug information.
- **Appliance Install log** – Displays internal debug information related to the installation process.

You can view the Event, Debug, and Install logs. The Debug and Install logs are intended for internal ARX use. When necessary, download them as instructed by ARX's technical support team and send them to ARX.

Starting from DocuSign Signature Appliance version 8.0, the Event Log is managed inside the appliance database. Upon a request to retrieve the event log, a zipped .csv file is returned.

Each event may contain the following information:

- Technical Identity (Number)
- Event Creation Time (Date-Time Number format) – as seconds from 1970
- Log Level – The event level of severity ,where 1 is the highest severity and 4 is the lowest severity
- Source – The internal technical module that initiated the event
- IP address – The IP address of the relevant client connecting to the appliance
- AdminTechID – The administrator's internal Tech ID
- AdminPrincipalName – The name of the relevant administrator
- UserTechID – The user's Internal Tech ID
- UserPrincipalName – The name of the relevant user
- EventID – An internal identification of the performed operation
- Value – A textual description of the event
- SignedData – In the case of a digital signature operation, this value is the hash representation of the data to be signed.

To view the Event log:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the desired DocuSign Signature Appliance appliance.
- From the popup menu, select **All Tasks** → **Download Logs** → **CoSign Event Log**.
- Select a file and click **OK**.
- Unzip the file to obtain a .CSV file.
- Use an application such as Excel or Notepad to view the .csv file.

Note: You can also download the event log by using the command line utility `GetEvt` (refer to [Using Command Line Utilities](#)).

Shutting Down and Restarting DocuSign Signature Appliance Services

You can stop and restart the DocuSign Signature Appliance internal services within the DocuSign Signature Appliance.

To stop and then restart the DocuSign Signature Appliance services:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the desired DocuSign Signature Appliance.
- From the popup menu, select **All Tasks** → **Restart** → **Soft Restart**.

Restarting the Appliance

There are several options for restarting or shutting down DocuSign Signature Appliance services and the DocuSign Signature Appliance:

- **Hardware Restart** – Restarts the appliance from a remote location.
- **Shutdown Appliance** – Shuts down the DocuSign Signature Appliance.

To restart or shut down the appliance:

- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click the desired DocuSign Signature Appliance appliance.
- From the popup menu, select **All Tasks** → **Restart** → **Hardware Restart/Shutdown Appliance**.

High Availability

In a high availability site, one appliance is defined as the *primary appliance*, and the other DocuSign Signature Appliances in the site are defined as *alternate appliances*. The following high availability options are available to the appliance administrator through the Administration MMC:

- **Install Alternate** – Install the alternate appliance software. Refer to [Installing the Alternate Appliance Software](#).
- **Subscribe Alternate to Primary** – Re-subscribe an existing installed appliance to be an alternate appliance of a selected primary appliance. Refer to [Resubscribing an Alternate Appliance with a Primary Appliance](#).
- **Set As Primary** – Set an existing alternate appliance to be the primary appliance. Refer to [Setting an Alternate Appliance to be the Primary Appliance](#).
- **Subscribe as Alternate** – If the existing cluster of appliances has more than one primary appliance due to recovery after failure, it is possible to set an appliance previously defined as the primary appliance to be an alternate appliance. Refer to [Setting a Previous Primary Appliance to be an Alternate Appliance](#).

Renewing the Subordinate CA Certificate

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

It is possible to install DocuSign Signature Appliance so that DocuSign Signature Appliance acts as a subordinate CA of another ROOT CA in the organization's environment. For more information on installing DocuSign Signature Appliance as a subordinate CA, refer to [Installing DocuSign Signature Appliance as a Subordinate CA](#).

If the certificate from the ROOT CA has expired or been revoked, you need to renew the certificate. It is recommended to start the renewal process at least a month before certificate expiration.

It is further recommended to adjust the renewal of the users' certificates to after the subordinate CA is renewed, but before it is expired, to avoid cases where an end-user's certificate is valid, but the CA certificate is not.

To renew the certificate when the CA is acting as a subordinate CA:

- In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the relevant DocuSign Signature Appliance and select **All Tasks** → **Subordinate CA** → **Download Certificate Request**.

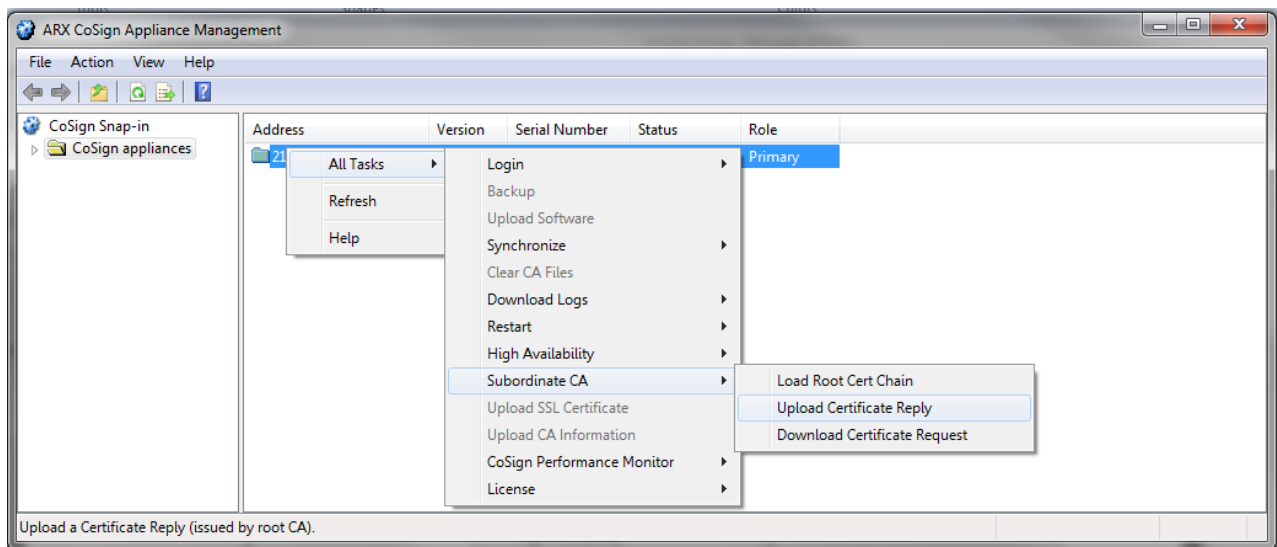


Figure 53 Subordinate CA Options

- A *File Selection* dialog box appears, prompting you to supply the name of the file that will contain the Certificate Request (CRQ) for DocuSign Signature Appliance as a subordinate CA.

DocuSign Signature Appliance will place the CRQ into this file.

- Submit the certificate request to the ROOT CA by providing the CRQ file.

The files you will eventually receive back from the ROOT CA include a group of files that constitute the complete chain of CA certificates, and the Certificate Reply file that contains the new subordinate CA certificate.

Note that if a ROOT CA certified DocuSign Signature Appliance, the complete chain of CA certificates includes only the ROOT CA certificate.

The subordinate CA certificate can also be packaged in certificate format (.cer) and not necessarily in a certificate reply format (.crp).

Note: Make sure that the certificate reply contains only the certificate and does not contain any of the certificates that are part of the certificate chain.
The certificates in the certificate chain are loaded separately.

Note: The file formats of the certificate and certificate chain must be ASN.1 (DER) encoded. If the files are encoded in BASE64 format, they must be converted.
If the subordinate CA certificate is encoded in BAES64 format, you can use the Microsoft standard certificate information utility to browse to that BASE64 certificate, and use the *copy to file* option to save the certificate to a DER encoded certificate.

- For each file in the chain of CA certificates, perform the following:
 - Right-click the relevant **CoSign appliance** and select **All Tasks → Subordinate CA → Load ROOT Cert Chain**.
A file selection window pops up.
 - Specify the path and file name of the CA certificate.

After each certificate is loaded, the following message appears: **Uploading root certificate chain finished successfully.**

- Right-click **CoSign appliances** and select **All Tasks → Subordinate CA → Upload Certificate Reply**.
A dialog box appears, prompting you to specify the Certificate Reply file, which contains the new subordinate CA certificate.
- Specify the path and file name of the Certificate Reply.

Note: In case of an error when uploading the new certificate, DocuSign Signature Appliance will continue running using its old CA certificate until the certificate expires.

Uploading an SSL Certificate

If DocuSign Signature Appliance is used in Web Services mode or RESTful based Web Services mode, access to Web Services is based on SSL security, that is, the SSL server must use a private key and a certificate. However, the DocuSign Signature Appliance is installed with a default SSL Server certificate pointing to an SSL Server with the name *cosign*. This default certificate would require that the organization configure each client as follows:

- Assign the IP address to the name *cosign*. (This can be done by updating the hosts file, located in `\windows\system32\drivers\etc` or in `\etc\hosts`).
- Trust the default certificate.

Instead, you can upload your own SSL Server Private Key and certificate which includes the DNS identification of the DocuSign Signature Appliance.

To upload your own SSL Server Private Key and certificate:

- Generate a private key and request a certificate from a well-known certificate authority.
- Upload the Private Key and Certificates chain that are packaged in a .pfx file to the DocuSign Signature Appliance.

When activating this option, a window pops up requesting you to supply the following:

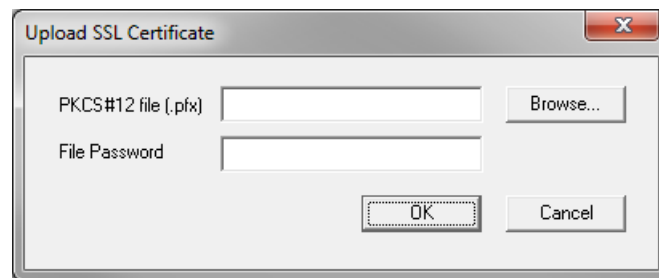


Figure 54 Upload SSL Certificate

- **PKCS#12 file (.pfx)** – Provide the file that includes the Private Key and Certificate chain.
- **File Password** – Provide the password that protects the Private Key in the PKCS#12 file.

This new Private Key and Certificate will replace the existing default Private Key and Certificate. The SSL Server will now use the Private Key and certificate for providing SSL communication based Web Services that match the organization network identities.

This operation will load the information to both a regular Web Services module and to a RESTful Web Services module.

Monitoring Performance Parameters of the Appliance

You can monitor the performance of the appliance. Use this option if the appliance has a heavy load and requires performance evaluation. Consult ARX support before activating this option.

Activating Performance Monitoring

To monitor appliance performance parameters:

- In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the relevant DocuSign Signature Appliance and select **All Tasks → CoSign Performance Monitor → Start Monitor**. The *Setup Performance Monitor Parameters* window appears.

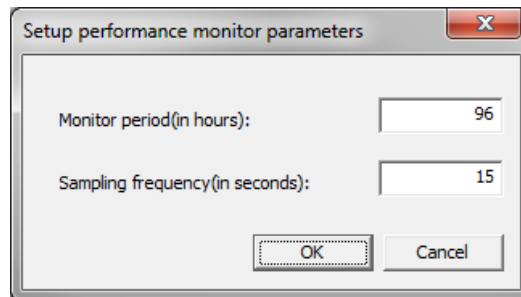


Figure 55 Setup Performance Monitor Parameters Window

- Specify the following:
 - **Monitor period (in hours)** – Specify the overall period of monitoring activity. When the monitoring period ends, the monitor service will stop.
 - **Sampling frequency (in seconds)** – Specify how often the monitoring service samples technical parameters.
- Click OK.

Monitoring begins. Monitoring will end at the end of the specified monitor period, or if you manually stop it as described in [Stopping Performance Monitoring](#).

Stopping Performance Monitoring

To stop monitoring of appliance performance parameters:

In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the relevant DocuSign Signature Appliance and select **All Tasks → CoSign Performance Monitor → Stop Monitor**.

Viewing Performance Parameters

To view the appliance performance parameters:

In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the relevant DocuSign Signature Appliance and select **All Tasks → CoSign Performance Monitor → Download Log**.

The downloaded file contains values for all sampled parameters. You can display the values in Excel. You can consult with ARX to evaluate whether the values are as expected.

Obtaining a New License

You can obtain a new license, while managing both the license request and the license response via email. This option is possible only if you have an existing license token. A new license is needed when you wish to change the number of end-users who may use the DocuSign Signature Appliance.

Requesting a New License

To request a new license:

- Make sure the license token is plugged into the USB slot in the DocuSign Signature Appliance.
- In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the relevant DocuSign Signature Appliance and select **All Tasks → License → Download License Request**.

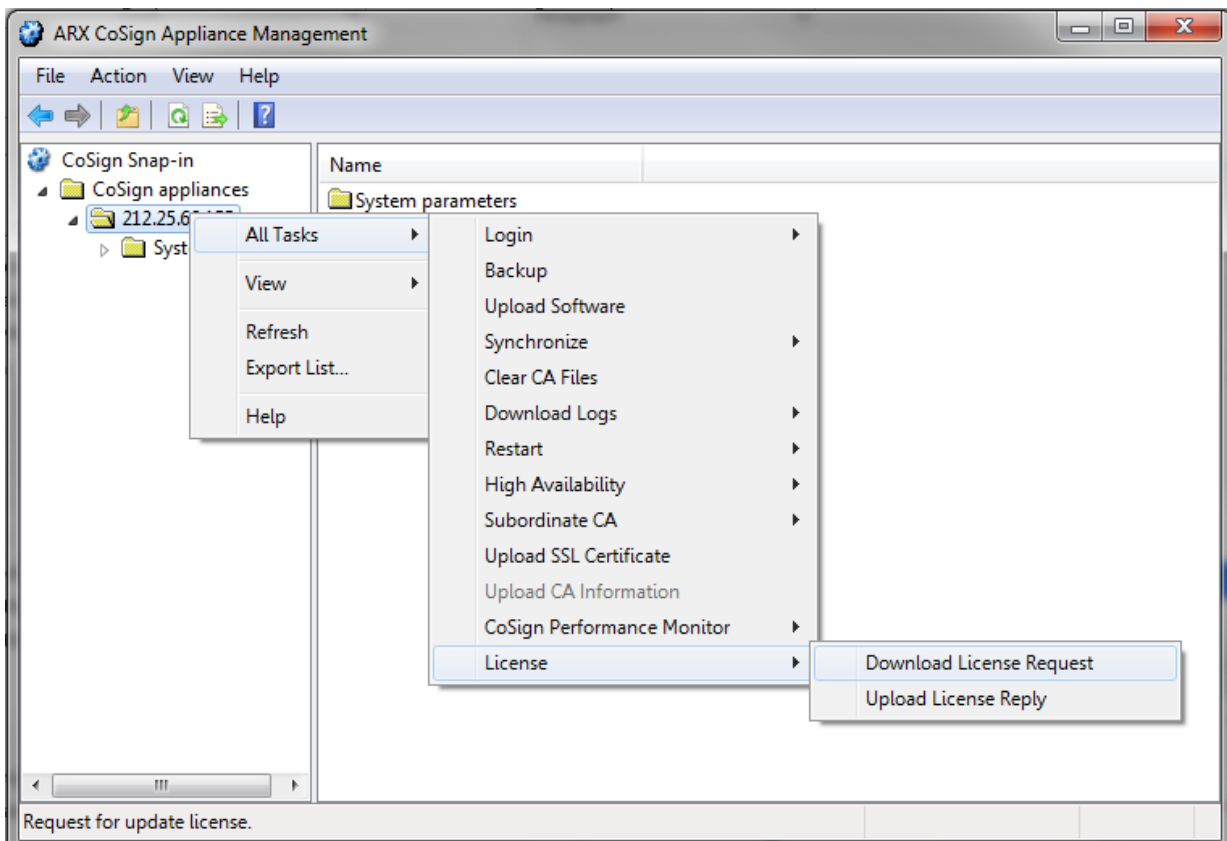


Figure 56 License Options

You are requested to provide a file path for the License Minikey Request (.lmr) file.

- Specify a location for the License Minikey Request (.lmr) file.
- Email the License Minikey Request (.lmr) file to your contact at ARX, and specify the requested number of signers.

Uploading the New License

ARX emails back a new license in the form of a License MiniKey Update (.lmu) file.

To upload the new license:

- Save the new .Imu license file on your system.
- In the *ARX CoSign Appliance Management* window ([Figure 51](#)), right-click the relevant DocuSign Signature Appliance and select **All Tasks** → **License** → **Upload License Reply** ([Figure 56](#)).
- Specify the .Imu license file.

The new license file is uploaded to the license token.

A message appears, informing you whether license upload was successful.

Changing System Parameters

You can easily change the various system parameters using the Administration MMC.

To change system parameters:

- In the left pane of the *ARX CoSign Appliance Management* window, click **System Parameters** for a specific appliance. The parameters are classified according to the context of the parameter. When you select a specific class of parameters, its parameters are displayed in the right pane, as shown in [Figure 57](#).

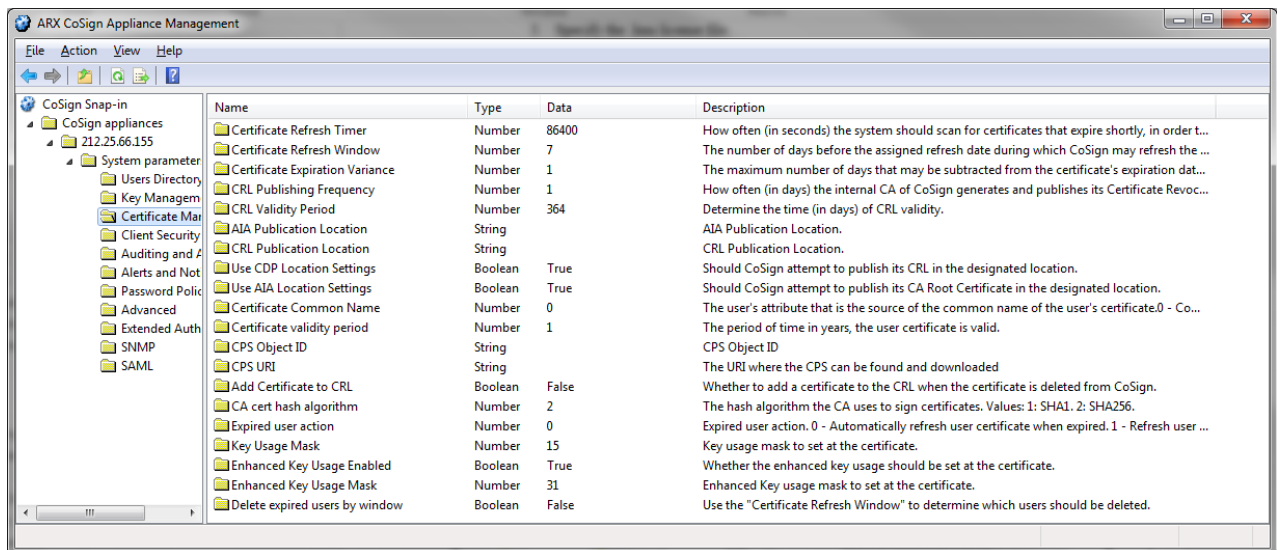


Figure 57 CoSign System Parameters

- Double-click a parameter to change the parameter's value. A popup dialog box appears with the parameter's current value.
- Change the value and click **OK**.

Note: You must perform a soft restart of the DocuSign Signature Appliance for the new parameter values to take effect (refer to [Restarting the Appliance](#)).

Note: In a High Availability configuration, you need to restart the alternate appliances as well.

The available parameters are listed below.

Users Directory Parameters

Note: This section is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

- **Group of CoSign Users (AD)** – The identification of the group in the Active Directory that defines the scope of DocuSign Signature Appliance users. This group is referred to as the *Signers Group*. This parameter is modifiable and defined during DocuSign Signature Appliance installation. This parameter should be provided in a Full Distinguished Name format, that is, *CN= CoSign Signers, CN = Users, DC= arx, DC=com*.

Note: Set this parameter with great care. All users who do not belong to the new Signers group will be deleted, as well as all their user information.

If DocuSign Signature Appliance is installed in a multiple domain environment, the Group name should not be entered in a Full Distinguished name format, but in a regular format as follows:
CoSign Signers.

- **Automatic Deletion of Users** – If this parameter is TRUE, DocuSign Signature Appliance automatically deletes a user from DocuSign Signature Appliance when the user is removed from the Signers group, or when the user's group is removed from the Signers group. This can be a problem if the administrator decides to temporarily remove the user from the Signers group. It is recommended to set this parameter to FALSE.

Default value: FALSE.

- **Appliance Administrator Group** – The name of the directory service's user group that identifies authorized DocuSign Signature Appliance administrators. Make sure that all users who perform DocuSign Signature Appliance administrative tasks are assigned to this group. You can choose any name for this group, under the following conditions:
 - In an Active Directory environment, provide the name of the administrative group (.e.g., administrators).
 - In an LDAP environment, provide this parameter in a Full Distinguish Name format, that is, *CN= Administrators, DC= arx, DC=com*.

Default value: administrators.

- **Users Administrator Group** – The name of the directory service's user group that identifies authorized DocuSign Signature Appliance user administrators. Make sure that all users who perform DocuSign Signature Appliance user administrative tasks are assigned to this group. You can choose any name for this group, under the following conditions:
 - In an Active Directory environment, provide the name of the administrative group, for example, *administrators*.
 - In an LDAP environment, provide this parameter in a Full Distinguish Name format, that is, *CN= Administrators, DC= arx, DC=com*.

Default value: administrators.

- **Directory Synchronization Timer** – How often (in seconds) the system should scan for updates in the directory service's user databases in order to generate keys and certificates for new users, update user certificates due to changes such as email address changes, or delete users.

Note: A low value (i.e., several seconds) increases DocuSign Signature Appliance synchronization with the directory service, but may decrease performance levels.

Default value: 40 seconds.

- **Create Group Keys** – Indicates whether a key and certificate are automatically generated for every group in the directory service. If this option is activated, every end user can digitally sign using his group certificates. If a user belongs to several groups, the user can use the certificates of all the groups to which the user belongs.

Note: If an External CA is used, use the `Groups.exe` utility. This utility enables the end user to define the current group. Any creation of keys and certificates by the end user will be automatically assigned to the current group.

Note: After updating this value and performing a soft restart of the DocuSign Signature Appliance, you must manually perform synchronization with the directory for generating keys and certificates for the directory groups.

Default value: False.

- **Create Computer Keys** – Indicates whether a key and certificate are automatically created for each computer in the directory service. This option is relevant for computer-based services that require signature operation. These services perform signature operations using the workstation's key.

Default value: False.

- **Periodic Directory Sync Timer** (LDAP and AD Multiple Domains environments) – How often (in seconds) the system should perform a full users database synchronization against the Directory's user databases in order to generate keys and certificates for new users, update user keys and certificates due to changes such as email address changes, or delete users. In the case of LDAP and AD Multiple Domains, synchronization only applies to user updates and user deletion.

Note: A low value (i.e., several seconds) increases the frequency of synchronization with the directory, but may decrease performance levels.

Default value: 1800 seconds.

- **User Certificate Publishing** (Active Directory) – Indicates whether to publish the end user's certificate to the user's account in the domain. This functionality is not necessary when certificates are used for signature operations.

Default value: False.

- **Directory Server Search Base** (relevant only for LDAP – This read-only field indicates the base location in the directory for searching the accounts of the signing users in the LDAP directory.

Default value: Empty.

- **Built-in CoSign Admin** (relevant for all environments except Directory Independent) – This Boolean parameter defines whether the only administrator of the system is the built-in administrator. That is, that there are no DocuSign Signature Appliance administrators from the domain, and the only administrator of the system is the built-in administrator. Setting this value to True improves the performance of any user login operation to the appliance.

Default value: False.

Key Management Parameters

Note: This section is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

- **Extractable Keys** – A read-only parameter. Specifies whether the generated keys of the users can be extracted from DocuSign Signature Appliance.

Note: DocuSign Signature Appliance cannot be configured to extract signature keys.

- **The Users Key Length** – The size in bytes of the users' keys. This is relevant if the internal CA is used.
If this parameter is changed, user keys and their certificates will be regenerated right after the appliance is restarted.
- **Regenerate user key** – If this parameter is set to True, private keys will be automatically regenerated upon certificate renewal.
If, upon certificate renewal, the new private key has a key size different from that of the original private key, a new private key will be regenerated regardless of the value of this parameter,
Default value: False
- **Create user key mode** – If this parameter is set to False, user keys will not be generated as part of the user creation process; rather, the keys will be created upon a user's first attempt to login.
Default value: False
- **Permit upload RSA keys** – If this parameter is set to False, the user cannot upload RSA keys into the DocuSign Signature Appliance and use them for signing data.
Note that if an external Certificate Authority is used, and during enrollment a key can be generated inside the DocuSign Signature Appliance as part of the enrollment process, then in this case the RSA key is generated inside the DocuSign Signature Appliance and not imported to the DocuSign Signature Appliance.
Default value: False
- **Maximum RSA key pool size** – If this parameter is set to a value larger than 0, the RSA key pool mechanism is activated.
In this mode, RSA keys are generated by the DocuSign Signature Appliance in advance so that when a key generation operation is performed (for example, in the case of generating a new account for a user), the operation will be performed instantly and an RSA key from the pool will be used instead of generating a new key.
If an RSA key Pool mechanism is required, it is recommended to specify the value **200,000**. This instructs DocuSign Signature Appliance to prepare 200,000 RSA keys in advance.

This functionality is not supported for cases where DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.
Default value: 0

Certificate Management Parameters

Note: This section is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

- **Certificate Refresh Timer** – How often (in seconds) the system should scan for certificates that expire shortly, in order to refresh the certificates.

Default value: 86400 seconds (24 hours).

- **Certificate Refresh Window** – The number of days before the assigned refresh date during which DocuSign Signature Appliance may refresh the certificate.

For example, if a certificate was assigned a refresh date of January 20 (based on the specified Certificate Expiration Variance), and the Certificate Refresh Window is 5 days, the certificate may actually be refreshed anywhere between January 16 and January 20.

Default value: 7 days.

- **Certificate Expiration Variance** – The maximum number of days that may be subtracted from the certificate's expiration date for the purpose of refreshing the certificate. This variance enables DocuSign Signature Appliance to spread the refresh activity over a number of days.

For example, if 1000 users are added on the same day, their certificates all expire on the same day as well. To avoid overloading the system on the expiration date, you might specify a variance of 10 days. DocuSign Signature Appliance would then assign a refresh date to each certificate (for example, 100 certificates on January 20, 100 on January 21, etc.).

Default value: 1 day.

- **CRL Publishing Frequency** – How often (in days) the internal CA of DocuSign Signature Appliance publishes its Certificate Revocation List (CRL) into Microsoft Active Directory.

Note: The CRL contains information regarding revoked users.

Default value: 1 day.

- **CRL Validity Period** – Determine the time (in days) that the generated CRL is valid.

Default value: 1 day.

- **AIA Publication Location** – This parameter can be modified. This parameter specifies the publication location of the AIA (Authority Information Access), which contains the Internal CA certificate.

This parameter is initially set during DocuSign Signature Appliance installation (refer to [Installing an Internal Certificate Authority](#)). If it is not set by the user, it retains its default value.

It is recommended to perform a Refresh Certificate operation (refer to [Refreshing Certificates](#)) after setting this parameter in order to include the updated parameter value in the generated certificate.

Note: Changing either the *AIA Publication Location* or the *CRL Publication Location* will automatically set both *Use CDP Location Settings* and *Use AIA Location Settings* to false. This means that if DocuSign Signature Appliance published the AIA or CDP to the domain, it will not continue and publish the certificate or CRL to the domain, and the administrator will need to find another mechanism for publishing the certificate or CRL.

- **CRL Publication Location** – This parameter can be modified. This parameter specifies the publication location of the CRL (Certificate Revocation List), which contains all the identifications of the revoked certificates of the CA.

This parameter is initially set during DocuSign Signature Appliance installation (refer to [Installing an Internal Certificate Authority](#)). If it is not set by the user, it retains its default value.

It is recommended to perform a Refresh Certificate operation (refer to [Refreshing Certificates](#)) after setting this parameter in order to include the updated parameter value in the generated certificate.

Note: Changing either the *AIA Publication Location* or the *CRL Publication Location* will automatically set both *Use CDP Location Settings* and *Use AIA Location Settings* to FALSE. This means that if DocuSign Signature Appliance published the AIA or CDP to the domain, it will not continue and publish the certificate or CRL to the domain, and the administrator will need to find another mechanism for publishing the certificate or CRL.

- **Use CDP Location Settings** – A read-only parameter. Specifies whether DocuSign Signature Appliance will attempt to publish the CRL in the specified location.

Default value: TRUE if the value of the *CRL Publication Location* parameter was not changed during installation. In a Directory Independent environment, the value of this parameter is always FALSE.

- **Use AIA Location Settings** – A read-only parameter. Specifies whether DocuSign Signature Appliance will attempt to publish the AIA in the specified location.

Default value: TRUE if the value of the *AIA Publication Location* parameter was not changed during installation. In a Directory Independent environment, the value of this parameter is always FALSE.

- **Certificate Common Name** – Defines how to set the value of the common name field in the user certificate.

0 – According to the common name field of the user in the directory.

1 – According to the display name field of the user in the directory.

Default value: 0.

- **Certificate validity period** – Defines the time in years that the end user's certificate is valid.

Default value: 1 year.

- **CPS Object ID** – Starting from CoSign 5, you can attach a certificate policy attribute to the certificate generated by the internal CA. The Certificate Policy Statement (CPS) contains a unique object ID (such as “2.16.840.1.113733.1.7.23.3”).

It is recommended to perform a Refresh Certificate operation (refer to [Refreshing Certificates](#)) after setting this parameter and the *CPS URI* parameter, to include the new parameter values in the generated certificate.

Default value: empty.

This parameter is mandatory if it is required to attach a CPS attribute to newly generated certificates.

- **CPS URI** – The URI of the location where the text of the CPS is published.

Default value: empty.

This parameter is mandatory if it is required to attach a CPS attribute to newly generated certificates.

- **Add Certificate to CRL** – Specifies whether to add certificates to CRLs when a user is deleted or his/her user data is updated.

Default value: false.

- **CA Cert Hash Algorithm** – The hash algorithm used in the certificate generation process by the internal CA.

A value of 1 means SHA-1. A value of 2 means SHA-256.

Default value: 2.

- **Expired user action** – This parameter is relevant when DocuSign Signature Appliance is deployed in very large user base scenarios (over 500,000 users). Please contact ARX before modifying this value.

The possible values include:

- **0 – automatically refresh user certificate when expired**
When a user certificate expires it is automatically refreshed. The relevant signature key can be refreshed as well depending on other system parameter values.
- **1 – Refresh user certificate at login**
Upon expiration, the user certificate will not be refreshed automatically but only when the user next logs in.
- **2 – Delete users with expired certificate**
In order to reduce utilization of database resources, user accounts will be deleted when their internal certificate is expired.

Default value: 2.

- **Key Usage Mask** – This parameter expresses the **Key Usage** value in the user certificate. The values are as defined in the **key usage** section of the X.509 standard as defined in RFC 5280.

Default value: 15.

- **Enhanced Key Usage Enabled** – Determines whether the user certificate includes an enhanced key usage attribute.

Default value: True.

- **Enhanced Key Usage Mask** – This parameter expresses the **Enhanced Key Usage** value in the user certificate.

Contact ARX support if you wish to modify this value.

Default value: 15.

- **Delete Expired users by window** – This parameter is relevant when DocuSign Signature Appliance is deployed in a very large user base scenario (over 500,000 users). Contact ARX if you wish to modify this value.

When this parameter is set to True, make sure that the [Expired user action](#) parameter is set to the value of 2. In this case, it means that user accounts will be deleted when their certificate is close to expiration (specifically, when it is X number of days away from expiration, where X is the value of the *Certificate Refresh Window* parameter).

When this parameter is set to False and the *Expired user action* parameter is set to the value of 2, it means the user account will be deleted when the user's certificate expires.

Default value: False.

- **External CA User Name** (Comodo) – The user name representing the organization that enables DocuSign Signature Appliance to interface the Comodo CA. Change this value only in accordance with ARX support.

Default value: as defined during installation.

- **External CA Password** (Comodo) – The password corresponding to the *External CA User Name*. Change this value only in accordance with ARX support.

Default value: as defined during installation.

Client Security Setting Parameters

- **Prompt for Logon** – Indicates whether the user gets a logon prompt (as shown in [Figure 58](#)) requiring entry of the user ID, password, and sometime their domain name, when logging on to DocuSign Signature Appliance. If set to TRUE, the following dialog box appears once, for every user login session in Windows.

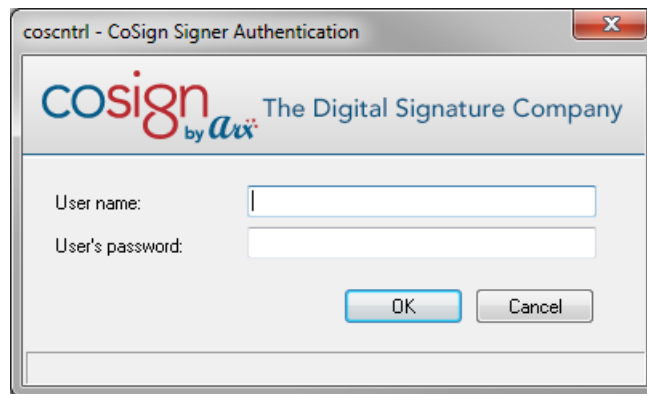


Figure 58 CoSign Logon Prompt

Note: In LDAP and Directory Independent environments, the **Prompt for Logon** parameter cannot be modified, and is automatically set to TRUE.

Note: If no input is entered into any of the logon dialog fields within the first 10 seconds, a 10-second timer appears in the dialog. If no input is entered by the time this timer expires, the logon dialog automatically disappears and the logon operation fails. This parameter can be changed via the Configuration Utility (refer to the *Configuration Utility* chapter in the *DocuSign Signature Appliance User Guide*).

Default value: False.

- **Prompt for Signature** – Indicates whether the user gets a prompt (as shown in [Figure 58](#)) requiring entry of the user's password before each digital-signature creation. When using extended authentication, this parameter must be set to True.

Note: The User ID and the domain name (if required) are displayed in the popup dialog box.

Note: In Common Criteria EAL4+ deployments this parameter is automatically set to True and cannot be modified.

Default value: False.

- **Enable Automatic User Logon** – This parameter is relevant for all modes that prompt a user to logon (i.e., Directory Independent, LDAP). If this parameter is True, then the user is able to access his/her public information such as the user certificate, without requiring a logon prompt. The logon prompt will appear only during a signature operation or a management operation such as uploading a new graphical signature.

Using this option, you can reduce the number of logon pop-ups in applications that only access the local store of users' certificates.

In the case of Active Directory installation when SSPI mode is used for authentication, setting this parameter to False will improve logon performance.

Default Value: True.

- **User Activation**– This parameter mandates user activation of his/her account prior to using the account.

In Common Criteria EAL4+ mode this parameter value is always True and cannot be modified. Please consult with ARX support before modifying this value.

Default Value: False.

Auditing and Accounting Parameters

- **Report Signatures to Event Log** – Indicates whether to report signature events to the event log. Disable this option only if very high performance rates are required.

Note: In Common Criteria EAL4+ deployments this parameter cannot be modified.

Default value: True.

- **Enable User Counters** – Indicates whether to enable user-based counters that enumerate signature operations.

Default value: False.

- **Report Apps Names To Event Log** – Indicates whether to record in the event log also the name of the client application that performed the digital signature operation.

Default value: False.

- **Event Log Storage Period** – Indicates the time in days that old events will be retained in the event log.

Default value: 7

Alerts and Notifications Parameters

- **Mail Server Name** – DNS name or IP address of the SMTP server used for sending email notifications.

Default value: No mail server

- **Mail Server Port** – The TCP/IP port number of the SMTP server used for sending email notifications.
Default value: 25.
- **Email From Address** – The source email address to be used for sending email notifications.
Default value: none.
- **Syslog Server IP Address** – The IP address of the syslog server. If the proper IP is set, all major events are also reported to the syslog server. Without entering the IP address, only events of system up or system down are reported to the syslog server.
Default value: 0.0.0.0 (No IP defined).

Password Policy

The following parameters are relevant to a Directory Independent environment. These parameters define a policy for the users' passwords.

- **Minimum Password Length** – The minimal password length of a DocuSign Signature Appliance user. The minimal length cannot be set to less than 6 characters.
Default value: 6.
- **Maximum Password Validity** – The maximal number of days the existing password is valid. A value of 0 indicates that the validity is indefinite.
Default value: 0.
- **Minimum Password Validity** – The minimal number of days the existing password is valid. During this period the password cannot be changed. A value of 0 means that this policy is not enforced.
Default value: 0.
- **Maximum Repeats in password** – The maximal number a character can be repeated in a password. A value of 0 means that the policy is not enforced.
Default value: 0.
- **Maximum Sequence in password** – The maximal number of ascending/descending characters in a password. A value of 0 indicates that this policy is not enforced.
Default value: 0.
- **User Must Change Password** – Whether the newly created user must change his/her password. In Common Criteria EAL4+ deployments, set this parameter to False. This causes the user activation process to mandate that each user set his/her own fixed password.
Default value: False.
- **Max Password Failed Attempts** – After the user failed to present his password several times, the user is locked and only an administrator can release the user by setting a new password. This field indicates the maximal number of failed attempts. A value of 0 indicates that this policy is not enforced.

LDAP

Note: This section is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

The following parameters are relevant to an LDAP based installation such as Sun-One, Tivoli, or OID environments. These parameters enable DocuSign Signature Appliance to properly communicate with the LDAP server for the purpose of user authentication and users synchronization.

- **Primary LDAP server address** – The DNS name or IP address of the primary LDAP server.
- **Primary LDAP server port** – The port number of the primary LDAP server.
- **Secondary LDAP server address** – The DNS name or IP address of the secondary LDAP server. This information enables DocuSign Signature Appliance to work in a High Availability directory environment.
- **Secondary LDAP server port** – The port number of the secondary LDAP server.
- **LDAP Authentication Method** – The method used to authenticate users in the LDAP Server.

0 – Simple Authentication. The user and password are sent in clear format.

1 – The password is sent using Digest MD5 format. If you specify this option, set *LDAP Secure Mode* to off.

Default value: 0.

- **LDAP Server Realm name** – The Realm name of the LDAP server, used when the authentication method is Digest-MD5. In a Sun One installation, this is the DNS name of the SUN One server.
- **LDAP Secure mode** – Whether secure LDAP is used or not. If this parameter is True, then secure LDAP is used, that is, both the user ID and the password are sent encrypted from DocuSign Signature Appliance to the LDAP server. Take care to also modify the LDAP Server port according to the secure LDAP port, which is in most cases port 636. To upload the Root Certificate of the SSL Server, use the *Subordinate CA\Load Root Cert Chain* option, and specify the ROOT certificate. If you specify LDAP secure mode, do not set *LDAP Authentication Method* to 1 (Digest-MD5 format).

Default value: False.

- **LDAP CoSign user name** – The full path distinguish name of a user who is allowed to query information from the LDAP directory. In some environment, such as SUN One, this definition is required by default. For example, in Sun One, a parameter such as the following should be provided:
`uid=administrator,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot.`
In other environments such as OID or Tivoli, this parameter can be left blank.
- **LDAP CoSign User Password** – The password of the user who can query users information in the LDAP server.
- **Search Base in LDAP Server** – The search base Distinguish Name for accessing information in the LDAP server.

- **LDAP Server UID attribute** – The name of the User ID attribute field in the LDAP server. If the value of this parameter is empty, this indicates that the default *uid* value is used. Consult with ARX before changing the value of this parameter.

Advanced Parameters

It is not recommended to modify any of the following parameters. Modify the parameters only if instructed to do so by ARX support.

- **CoSign Debug Level** – Modify this parameter only when instructed to do so by ARX’s technical support team.

Note: Running in debug mode (i.e., Debug Level is greater than 2) significantly decreases performance levels.

Default value: 2.

- **Clients Inactivity Timeout** – The time period after which DocuSign Signature Appliance disconnects inactive clients, in seconds.

Note: In environments with thousands of DocuSign Signature Appliance clients, it is recommended to decrease this value to several minutes. This reduces usage of appliance resources by DocuSign Signature Appliance clients.

Default value: 7200 seconds (2 hours).

- **Use SSL Proxy** – Set this parameter to true if the DocuSign Signature Appliance can connect to the Internet only through an SSL proxy. This parameter is necessary if the DocuSign Signature Appliance must connect to a World Wide Verifiable CA to get users’ certificates.

Default value: false.

- **SSL Proxy IP** – If DocuSign Signature Appliance is installed in an organization which allows access to the internet only through an HTTP proxy, DocuSign Signature Appliance can be configured to use this proxy when accessing external services such as the automatic external CA. Indicates the IP address of the organization’s HTTP proxy.

Note that modifying this parameter requires a hardware restart of the DocuSign Signature Appliance.

Default value: empty.

- **SSL Proxy Port** – If DocuSign Signature Appliance is installed in an organization which allows access to the internet only through an HTTP proxy, DocuSign Signature Appliance can be configured to use this proxy when accessing external services such as the automatic external CA. Indicates the port number of the organization’s HTTP proxy.

Note that modifying this parameter requires a hardware restart of the DocuSign Signature Appliance.

Default value: empty.

- **SSL Proxy User Name** – If the HTTP proxy through which the organization accesses the internet requires authentication, this field indicates the valid user name of a user in the organization.

Note that modifying this parameter requires a hardware restart of the DocuSign Signature Appliance.

Default value: empty.

- **SSL Proxy Password** – If the HTTP proxy through which the organization accesses the internet requires authentication, this field indicates the password corresponding to the user name of a user in the organization

Note that modifying this parameter requires a hardware restart of the DocuSign Signature Appliance.

Default value: empty.

- **Web Services Support** – Indicates whether the DocuSign Signature Appliance provides a Web Services interface. The Web Services interface runs on port 8080 of the DocuSign Signature Appliance. In Common Criteria EAL4+ mode or FIPS 140-2 level 3 mode, this interface should be closed; that is, set this parameter to False.

Default value: true.

- **RESTful Web Services Support** – Indicates whether the DocuSign Signature Appliance provides a RESTful Web Services interface. This interface runs on port 8081 of the DocuSign Signature Appliance.

Default value: true.

- **CORS domain for REST API** – The RESTful API can be called as part of an HTTP session of another domain. For example, JavaScript code that is used as part of a Web Session from another domain can interface with the REST API. In these cases, this system parameter can be set to enable interacting with the RESTful API from specific domains using a semicolon separated string. For example: eg1.com;eg2.com.

- **Enforce FIPS Approved Algorithms** – If this parameter is set to True, then only RSA keys that are equal to or bigger than 2048 bits can be used, and only SHA2 algorithms (SHA256, SHA384 or SHA512) can be used for the digital signature operation.

Set this parameter to True if you would like DocuSign Signature Appliance to operate in FIPS mode.

When DocuSign Signature Appliance is installed in a Common Criteria EAL4+ mode of operation, this parameter is set to True and cannot be changed.

Default value: false.

- **Case Sensitive Username** – This parameter is relevant for a Directory Independent installation. Prior to CoSign version 6, login usernames were case sensitive. Starting from version 6, by default login usernames are case insensitive. It is not possible to change this value after the appliance is installed. If you wish to change the value, set it in the Configuration Utility prior to installation (refer to [Admin – Appliance Installation](#)). Note that when you perform an upgrade, the value of this parameter does not change because all installations prior to version 6 are always case sensitive.

Default value: false (case insensitive).

- **Allow Get Backup anonymously** – In this parameter an IP address can be specified to enable downloading an automated backup of the DocuSign Signature Appliance without supplying an administrator user ID and a password.

The backup process can be performed from the specified IP address.

An IP address of 0.0.0.0 indicates that it is not possible to get the backup without supplying a user ID and a password.

Default value: 0.0.0.0.

- **Common Criteria Mode** – This parameter indicates whether DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode. If it is, the parameter has a value of True.
- **Common Criteria Type** – This parameter indicates the type of Common Criteria EAL4+ mode. It can have one of the following values:
 - 0 – DocuSign Signature Appliance is installed as a Signature Creation Device
 - 1 – DocuSign Signature Appliance is installed as a Seal Creation DeviceThis value cannot be changed after the appliance is installed.
- **Cloud Monitoring** – This value indicates the type of monitoring used for sending information to a Cloud Monitoring system. It can have the following values:
 - 0 – Not activated
 - 1 – Production based cloud monitoring. Should be used when the appliance is in the production stage.
 - 2 – Test based cloud monitoring. Should be used when the appliance is undergoing testing.

Default value: 0

- **Cloud Site ID** – a string identification value that should be configured if instructed to do so by ARX Support.

Default value: empty

Extended Authentication

The following parameters are relevant in cases where the regular user authentication during signature operation is extended to use one of the following mechanisms:

One Time Password using a Radius Server – The end user enters a One Time Password (OTP) using a special device. The One Time Password is checked against a Radius Server, external to the DocuSign Signature Appliance.

The parameters described in [Extended Authentication - Radius](#) enable DocuSign Signature Appliance to communicate with the Radius Server.

- **Smart Card Authentication** – The user is requested to use a SmartCard as part of the signature approval. As part of the digital signature operation, the DocuSign Signature Appliance approves a Challenge that is signed by the SmartCard. The parameters described in [Extended Authentication - SmartCard](#) enable DocuSign Signature Appliance to communicate with the SmartCard. To upload the Root Certificate of the authentication certificate of the end user, use the *Subordinate CA\Load Root Cert Chain* option and specify the ROOT certificate
- **Biometric Authentication** – An approval is sent to the DocuSign Signature Appliance as part of the biometric authentication. The parameters described in [Extended Authentication - Biometric](#) enable DocuSign Signature Appliance to communicate with the biometric device.

Keep in mind that in extended authentication, the Prompt for Signature parameter must be set to True (refer to [Client Security Setting Parameters](#)).

Extended Authentication - General

- ***Extended Authentication Method*** – Define the primary authentication method to be used:
 - 0 – Built in: No extended authentication method. DocuSign Signature Appliance uses the regular password verification mechanism.
 - 1 – Radius based extended authentication.
 - 2 – SmartCard based extended authentication.
 - 3 – Biometric based extended authentication.

When DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode as a Qualified Signature Creation Device, the value is always 1 and cannot be modified.

When DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode as a Qualified Seal Creation Device, the value is always 0 and cannot be modified.

Default: 0.

- ***Alternate Extended Auth mode*** – When defined, if there is a problem during extended authentication, then the DocuSign Signature Appliance will try using an alternate method.
 - 1 – None: DocuSign Signature Appliance rejects the authentication attempt.
 - 0 – Built in: No extended authentication method. DocuSign Signature Appliance uses the regular user password.
 - 1 – Radius based extended authentication.
 - 2 – SmartCard authentication based extended authentication.
 - 3 – Biometric based extended authentication.

Default: -1.

Note: this parameter is not implemented.

Extended Authentication - Biometric

- ***Biometric Authentication Window*** – For information contact ARX.
- ***Biometric Shared Secret*** – For information contact ARX.

Extended Authentication – SmartCard

Note: This section is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

- ***SmartCard Authentication Window*** – The SmartCard authentication is based on a challenge that is signed by the end user's SmartCard. The challenge is based on time, which is verified by the DocuSign Signature Appliance. The Authentication window is the time in seconds that can elapse from the actual signature time.

Default: 120.

- ***Use SmartCard Auth for Logon*** – Determines whether the login will also be based on SmartCard authentication. This option is relevant mostly for Active Directory deployments that require only a SmartCard for login operation.
 - 0 – Login is not based on SmartCard authentication.
 - 1 – Login is based on SmartCard authentication.

Default: 0.

- **Certificate Issuer Name** – Validate users who are certified by the specified issue name. If this parameter is empty then any ROOT certificate trusted by the DocuSign Signature Appliance can certify users.
- **Enforce CRL Validation** – Indicates that the DocuSign Signature Appliance will always check the CRL. If there is any access problem to the CRL, the user authentication will fail.
- **CRL Retrieval** – Assists the certificate validation mechanism of the SmartCard authentication certificate.
When querying the CRL, this parameter indicates whether to retrieve the CRL from the cache, or it indicates the timeout when retrieving the CRL from the network.

0 – Use the default timeout value for retrieving the CRL from the network.

1 – Retrieve the CRL from the CRL Cache.

Other – A timeout in milliseconds for retrieving the CRL.

Default: 0

Extended Authentication - Radius

- **Require Static Password** – When this value is true, the end user must enter the static password, followed immediately by the Radius password.

If the Radius server has an internal mechanism that combines a static password and a dynamic password, it is advisable to set this parameter to False. In addition, do not get confused between the static password assigned by the Radius server and the static password required by the DocuSign Signature Appliance

In Common Criteria EAL4+ mode when DocuSign Signature Appliance is installed as a Qualified Signature Creation Device, this parameter is always True and cannot be modified.

Default: False.

- **Default Radius password length** – If *Require Static Password* is set to True, this parameter specifies the number of characters in the Radius password. This enables the DocuSign Signature Appliance to separate the regular password from the Radius password.

DocuSign Signature Appliance will authenticate the user using the static password, and then send only the Radius password portion to the Radius server for authentication.

Default: 6.

- **Radius Server IP Address** – The IP address of the Radius Server.
- **Radius Server port** – The port number of the Radius Server.

Default: 1812.

- **Alternate Radius Server IP Address** – This parameter is not applicable.
- **Alternate Radius Server Port** – This parameter is not applicable.

Default: 1812.

- **Radius Server Secret** – The shared secret between the Radius Server and the DocuSign Signature Appliance appliance.

- **Radius Server Timeout** – The time in seconds to wait for the Radius server’s response.
Default: 5.
- **Radius Server Retries** – The permitted number of retries when trying to validate the user credentials against the Radius server.
Default: 2.
- **Enable the Radius AD attribute** – If set to True, the user identification that is sent to be approved by the Radius server is based on the value of the *Radius customer AD attribute* parameter.
This parameter is only relevant when DocuSign Signature Appliance is installed in an Active Directory environment.
Default: False.
- **Radius custom AD attribute** – The name of the attribute in the Microsoft Active Directory to be used as a user identity sent to the Radius server. For example, **physicalDeliveryOfficeName**. If the content of the field is empty and the value of *Enable the Radius AD attribute* is True, the user will be rejected.
This parameter is only relevant when DocuSign Signature Appliance is installed in an Active Directory environment.
- **OTP validation method** – This parameter defines the OTP device types that can be used. The following types can be used:
 - 1 - OATH-HOTP – a standard OATH-based OTP device that is an event based OTP.
 - 2 - OATH-TOTP – a standard OATH-based OTP device that is a time-based OTP.
 - 3 - VASCO – An OTP devices manufactured by Vasco.
- **OTP OATH validation window** – This parameter is relevant when an OATH-HOTP device is used (an event based OTP device). The validation window enables validating several validation events for cases where the end user pressed the Event button several time before using it for the current digital signature operation.
- **Additional Radius IPs (CC Mode)** – Relevant for the case where Radius Servers are used in a High Availability configuration, and where a special switch is used to select which Radius Server to use. In Common Criteria (CC) Mode, the Radius callback can be called from a list that is composed of the above [Radius Server IP Address](#) and a list of semicolon-separated IP addresses. For example: 10.0.0.1;20.0.0.1
- **Login for Sign Window** – The value is defined in seconds.
If this parameter is set to a value larger than 0, then several digital signatures can be performed from the same application following successful authentication.
The only constraint is that the digital signature operations must occur within the defined time window.
A value of 0 indicates that authentication is required for every signature operation.
Default value: 0

SNMP

The SNMP protocol is used for sending SNMP traps or setting SNMP parameters for viewing the activity and performance status of the appliance.

- **SNMP Service** – Defines whether the SNMP service is on or off.

If the SNMP Service is on, the DocuSign Signature Appliance can be used by a monitoring server to inspect information.

The MIB identity of the software is **1.3.6.1.4.1.2774.3.1**, where the prefix **1.3.6.1.4.1.2774** specifies the vendor of the product.

Default: False.

- **SNMP Accepted community name** – Defines which community members can manage the SNMP agent. This parameter is concealed.

- Default: Empty.

- **SNMP Manager 1** – An IP address of the first SNMP management system.

- Default: Empty.

- **SNMP Manager 2** – An IP address of the second SNMP management system.

Default: Empty.

- **Contact Name** – The contact name of the SNMP agent residing in this DocuSign Signature Appliance.

Default: Empty.

- **Location** – The location name of the SNMP agent residing in this DocuSign Signature Appliance.

Default: Empty.

SAML

You can connect to DocuSign Signature Appliance and present an SAML ticket provided by a trusted organizational server.

Note: The following SAML parameters are not relevant when DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.

- **SAML Working Method** – The SAML authentication mode used for Logon operation. The possible values include:
 - 0 – Disabled – It is not possible to present an SAML token as part of the user login process.
 - 1 – All Users – All users can present an SAML token as part of their initial connection to the service and in subsequent login operations.
 - 2 – User with group association – Only users who are associated with a DocuSign Signature Appliance group can present an SAML token as part of their initial connection to the service and in subsequent login operations.

- ***Accepting Relying Parties Tickets*** – The name of the service as identified by the relying parties that generate the SAML tickets. The service can be specified based on a regular expression. If there are several regular expressions they can be separated by a semicolon.
- ***SAML Common Name*** – The name of the attribute in the SAML ticket that stores the end user's common name.
Default: CommonName.
- ***SAML Email Address*** – The name of the attribute in the SAML ticket that stores the end user's email address.
Default: emailaddress.
- ***SAML UPN*** – The name of the attribute in the SAML ticket that stores the end user's identity.
Default: upn.
- ***SAML Telephone Number*** – The name of the attribute in the SAML ticket that stores the end user's telephone number.
Default: telephoneNumber.
- ***SAML Display Name*** – The name of the attribute in the SAML ticket that stores the end user's Display Name.
Default: displayName.
- ***SAML Group Name*** – The name of the attribute in the SAML ticket that stands for the end user's Group. In order to utilize the Group functionality of DocuSign Signature Appliance, the SAML group name must match an existing group defined in the DocuSign Signature Appliance appliance.
Default: Group.
- ***SAML Window*** – The grace period in minutes during which the SAML ticket is still valid beyond the formal expiration time of the SAML ticket, as well as the time period in minutes that the SAML ticket is valid before the formal starting time of the SAML ticket. This parameter is intended to solve time synchronization issues.
Default: 5 minutes.

Restoring the Appliance

The Restore operation enables you to restore the appliance from a previously generated backup file (refer to [Backing up the DocuSign Signature Appliance Data](#)). You may wish to do this if there has been data loss or corruption or if you want to set up a new appliance with the data from a previously installed appliance.

The Restore operation is similar to installation (refer to [Installing the Appliance Software](#)). However, since a backup file is used for restoration, not all information entered during installation needs to be reentered. In addition, the restore operation usually takes less time than installation. The actual length of time depends on the number of users who were created/deleted/updated after the date of the backup, and the selected key length.

The following sections provide instructions for restoring the DocuSign Signature Appliance in Microsoft Active Directory, LDAP, and Directory Independent environments.

Restoring the Appliance in Microsoft Active Directory

Note: In order to run the restore operation, you must have permissions similar to those required for installing the appliance software. Refer to [Installing the Appliance Software](#) for more information.

To restore the appliance:

- Make sure the appliance is in Factory Settings mode. You can check whether the **Install** state is **Factory** in the consoles' **Status** menu (refer to [Displaying Status](#)). To restore DocuSign Signature Appliance to its factory settings, refer to [Restoring Factory Settings](#).
- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click **CoSign appliances** and select **All Tasks** → **Restore** from the popup menu. A standard file selection dialog box appears.
- Browse to the backup file, and click **Open**.
- Enter the IP address of the DocuSign Signature Appliance and click **Next**. The User setup dialog box appears.
- Click **Next**. Enter the built-in administrative user. You must provide the password of the built-in administrative user and confirm the password.
- Enter the **Admin user name** and **Admin password** of an administrator who has **permission to join the CoSign appliance to the domain**.

Note: The **Admin user name** enables DocuSign Signature Appliance to register computers as members of the domain during restoration. DocuSign Signature Appliance does not require these administrative rights for regular use.

In the following pages, default settings from the original installation will appear disabled. Click **Next** at every page.

- Click **Next**. DocuSign Signature Appliance restoration begins. A status bar displays the status of the restore operation.
- At the prompt, insert the backup MiniKey token that was used when first installing this appliance. DocuSign Signature Appliance reads the data from the MiniKey token. No writing to the MiniKey token is performed at this stage.

- At the prompt, insert the license MiniKey token.

When the operation is complete, the message `Installation of CoSign appliance finished successfully` appears above the status bar.

Note: It is highly recommended to restart the DocuSign Signature Appliance and synchronize DocuSign Signature Appliance with the Active Directory immediately after restoring the DocuSign Signature Appliance. For more information, refer to [Synchronizing DocuSign Signature Appliance with the Directory Service](#).

Restoring the Appliance in an LDAP Environment

To restore the appliance:

- Make sure the appliance is in Factory Settings mode. You can check whether the **Install** state is **Factory** in the consoles' **Status** menu (refer to [Displaying Status](#)). To restore DocuSign Signature Appliance to its factory settings, refer to [Restoring Factory Settings](#).
- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click **CoSign appliances** and select **All Tasks** → **Restore** from the popup menu. A standard file selection dialog box appears.
- Browse to the backup file and click **Next**.
- Enter the IP address of the appliance.
- Click **Next**. Enter the built-in DocuSign Signature Appliance administrative user. You must provide the password of the built-in administrative user and confirm the password.

In the following pages, default settings from the original installation will appear disabled. Click **Next** at every page.

- Click **Next**. DocuSign Signature Appliance restoration begins. A status bar displays the status of the restore operation.
- At the prompt, insert the backup MiniKey token that was used when first installing this appliance. DocuSign Signature Appliance reads the data from the MiniKey token. No writing to the MiniKey token is performed at this stage.
- At the prompt, insert the license MiniKey token.

When the operation is complete, the message `Installation of CoSign appliance finished successfully` appears above the status bar.

Restoring the Appliance in a Directory Independent Environment

To restore the appliance:

- Make sure the appliance is in Factory Settings mode. You can check whether the **Install** state is **Factory** in the consoles' **Status** menu (refer to [Displaying Status](#)). To restore DocuSign Signature Appliance to its factory settings, refer to [Restoring Factory Settings](#).
- In the ARX CoSign Appliance Management window ([Figure 51](#)), right-click **CoSign appliances** and select **All Tasks** → **Restore** from the popup menu. A standard file selection dialog box appears.

- Browse to the backup file and click **Next**.
- Enter the IP address of the appliance and click **Next**. The *User setup* dialog box appears.
- Click **Next**. Enter the built-in DocuSign Signature Appliance administrative user. You must provide the password of the built-in administrative user and confirm the password.

In the following pages, default settings from the original installation will appear disabled. Click **Next** at every page.

- Click **Next**. DocuSign Signature Appliance restoration begins. A status bar displays the status of the restore operation
- At the prompt, insert the backup MiniKey token that was used when first installing this appliance. DocuSign Signature Appliance reads the data from the MiniKey token. No writing to the MiniKey token is performed at this stage.
- At the prompt, insert the license MiniKey token.

When the operation is complete, the message `Installation of CoSign appliance finished successfully` appears above the status bar.

Using the Users Management Utility

The `Users Management` utility provides user management operations in cases where DocuSign Signature Appliance is installed in a Directory Independent environment as well as the ability to view and perform some actions upon users when DocuSign Signature Appliance is installed in Active Directory /LDAP environments.

The `Users Management` utility enables an administrator to perform the following:

- Add a new user (only in a DI environment).
- Delete an existing user (in an LDAP, Multiple AD Domains, and DI environment).
- Change the password of an existing user (only in a DI environment). Note that this operation is not allowed when DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.
- Enable a user to log in to DocuSign Signature Appliance or disable a user from logging in to DocuSign Signature Appliance.
- View users' information.
- Reset global and user-based signature counters.

You can also define groups of users. A user can be assigned to one group at most. The group's settings affect all users who are members of that group; for example, if a group is disabled, all users who belong to the group cannot login to DocuSign Signature Appliance.

The groups mechanism is available only in Directory Independent installations.

An organization can use the groups mechanism to define multiple user communities that are served by a single DocuSign Signature Appliance. Each group's settings specify the rules and parameters for managing that group of users.

It is also possible to manage Active Directory users in DocuSign Signature Appliance groups by assigning each user to a group after the user is copied from the Active Directory to DocuSign Signature Appliance.

When SAML is used, a user that initially connects to the DocuSign Signature Appliance by presenting a SAML ticket is automatically assigned to a group if the SAML ticket contains a Group attribute.

Group management is not enabled when DocuSign Signature Appliance is installed in a Common Criteria EAL4+ mode of operation.

The `Users Management` utility enables the administrator to perform the following group-related actions:

- Add a new group
- Delete an existing group
- Update an existing group
- View a group's settings
- Assign a user to a group or unassign a user from a group.

Note: All these operations can be performed using a DocuSign Signature Appliance API called Signature Local User Management API. For more information on DocuSign Signature Appliance Signature APIs, refer to the *DocuSign Signature Appliance Signature APIs Developer's Guide*.

Activating the Users Management Utility

The `Users Management` utility is installed as part of the `ARX CoSign Admin` client component.

To activate the `Users Management` utility:

- Open the **Start** menu and select **Programs** → **ARX CoSign** → **CoSign Control Panel**. The Control Panel appears.
- In the control panel activate the `Users Management` utility.

The `Users Management` main window appears.

- Use the **Login** or **Login built-in user** option to enable the administrator to login to DocuSign Signature Appliance.
- Click **Login** and enter your user-name and password.

The user-name and password is verified by the DocuSign Signature Appliance. Also, the DocuSign Signature Appliance checks that the connecting user has user administration access rights.

Users Management Main Window

The main window of the `Users Management` utility displays existing users in the DocuSign Signature Appliance database. Management operations can be performed using the drop-down menus, the toolbar, or the right click menu that appears when a user is selected.

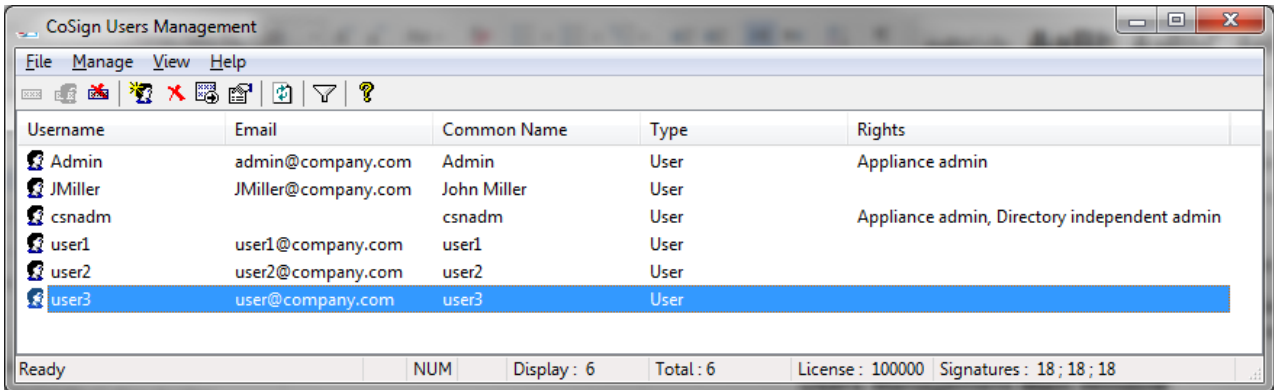


Figure 59 Directory Independent Users Management Utility - Main Window

The following user details can be displayed:

- **User Name** – The login name of the user.
- **Email** – The email address of the user.
- **Common Name** – The common name of the user.
- **Type** – The type of user: User, Computer, Group. The Computer and Group types are relevant when working with Computer Keys or Group Keys (refer to [Users Directory Parameters](#)).
- **Rights** – The access rights of the user. The following rights are possible:
 - Regular user.
 - Appliances admin.
 - Users admin.
 - Group admin.

Note:

Only a Users admin can create new users and assign roles to a user. This means that only a Users admin can create an Appliances admin.

The Appliances admin cannot add permissions to existing users.

When DocuSign Signature Appliance is deployed in Common Criteria mode, you cannot create a user who has both administrative privileges and signatory/user privileges.

- **Last Update Time** – The date and time when the user was last updated.
- **User Status** – The current status of the user. The possible values are:
 - Enabled.
 - Disabled. In the case of an Active Directory environment, this indicates that the user was removed from the Signers group in Microsoft Active Directory. The user still exists in the DocuSign Signature Appliance users database, but is not able to sign. In the case of a Directory Independent environment, this indicates that the user cannot login to DocuSign Signature Appliance.

- **Signature Counter** – Counts how many signatures the user performed. The counter is effective only if the **Enable User Counters** system parameter is set to True.
- **Enrollment Status** – The enrollment status of the user's certificate.
- **Enrollment reason** – Reason for certificate enrollment.

Users Management Window Status Bar

The status bar of the Users Management window displays the following information:

- **Display** – The number of users currently in the display. If a filter is used, the number will include only the users that matched the filter and appear on screen.
- **Total** – The number of users in the DocuSign Signature Appliance database.
- **License** – The number of users in the license token of the DocuSign Signature Appliance.
- **Signatures** – The number of digital signatures that were performed using the DocuSign Signature Appliance. Three signature counters are displayed. The second and third counters can be reset by the administrator. The first counter cannot be reset and displays the overall number of digital signature operations performed by the appliance since it was installed.

Users Management Menus

The following sections describe the menu options available from the `Users Management` drop-down menus: **File**, **User**, **View** and **Help**.

File Menu

The following options are available from the **File** drop-down menu.

Reset System Signature Counter

Enables the administrator to reset the second and third system signature counters. Each of these counters displays the number of signatures performed using DocuSign Signature Appliance since the counter was last reset.

Generate Users report

Enables generating a report for all DocuSign Signature Appliance users. This report contains all the important DocuSign Signature Appliance user record fields. The report is output in a format that can be displayed in Microsoft Excel.

Login

Enables the administrator to login to DocuSign Signature Appliance. The administrator is prompted for his/her user ID and password. If DocuSign Signature Appliance is installed in an MS Active Directory and the mode of operation is SSPI, the administrator is logged on based on the existing PC login session.

Login built in user

Enables login using the built in administrator. The administrator is prompted to provide a user ID and password.

Logout

Enables the administrator to logoff DocuSign Signature Appliance.

Exit

Closes the *Users Management* application.

Manage Menu

The following options are available from the **Manage** drop-down menu. The options are activated upon a selected user.

Reset User signature counter

Enables resetting the first and second signature counters of the user.

Reset User Password Counter

If a user's password is locked due to presenting a wrong password in multiple login attempts, an administrator can unlock the user account so that the user can try logging in again.

Note that this option merely resets to zero the number of actual failed login attempts.

New User

This option is relevant only when DocuSign Signature Appliance operates in a Directory Independent environment. This option enables adding a new user to DocuSign Signature Appliance. When this option is selected, the *New User* dialog box appears.

Figure 60 *Users Management Utility – New User Dialog Box*

Enter the following user parameters:

- **User Name** – The identification of the new user.
- **Common Name** – The Common Name of the user as it will appear in the user's certificate.
- **Email** – The email address of the user, as it will appear in the user's certificate.
- **Permissions** – The user's authorizations. Select one or more of the following:
- **User** – A regular DocuSign Signature Appliance user.

- **Appliances Management** – Permission to perform administrator activities, such as downloading the event log and backing up the database.
- **Users Management** – Permission to manage DocuSign Signature Appliance users.
- **Group Management** – Permission to manage users in the group to which this user belongs.

When DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode, a user cannot be both an administrator (of either type) and a regular user.

- **Password** – The password of the user.
- **Confirm Password** – Confirmation of the user's password.
- **Group** – The group to which the user is assigned. If you click **Select**, the *Manage Groups* dialog box appears, enabling you assign a user to any group, or to none.

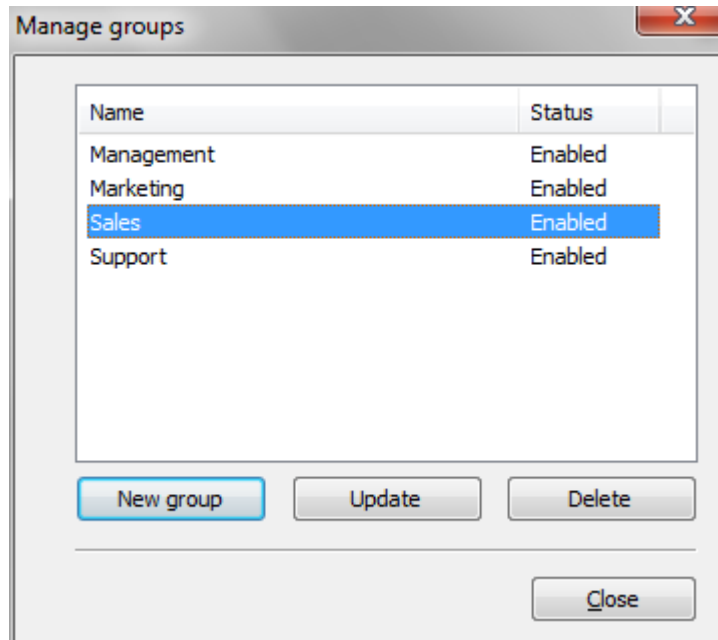


Figure 61 Manage Groups Dialog Box

Delete User

Enables deleting a user from the DocuSign Signature Appliance. When this option is selected, a confirmation message appears, requiring confirmation for the deletion operation.

Set User Password

Enables updating a user's password. When this option is selected, the *Set new password* dialog box appears. Enter and confirm the new password.

Note that this dialog box also enables the administrator to update the permissions of the user.

Note that setting a password is not possible when DocuSign Signature Appliance is installed in Common Criteria EAL4+ mode.

User Properties

Enables displaying existing information for a selected user. When this option is selected, the *User Data* dialog box appears.

Username:	JMiller
Common Name :	John Miller
Email :	JMiller@company.com
Type :	User
Permissions :	<input checked="" type="checkbox"/> User <input type="checkbox"/> Appliances Management <input type="checkbox"/> Users Management <input type="checkbox"/> Group Management
Last Update Time :	Wed Mar 02 14:36:11 2016
Status :	Enabled
General Signatures Counter :	0
Personal Signature Counter 1 :	0
Personal Signature Counter 2 :	0
Group:	Select...
Enrollment Status :	Certificate is OK

Figure 62 Users Management Utility – User Data Dialog Box

Note that almost all properties can be viewed in the main window of the users Management utility. The Personal Signatures Counter 1 and Personal Signature Counter 2 displayed in this dialog box indicate the number of digital signature performed by this user since the last time these counters were reset for the user. These counters are active only if the *Enable User Counters* system parameter is set to True.

Manage Groups

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

This option displays the *Manage Groups* dialog box. Using this dialog box you can manage all groups inside DocuSign Signature Appliance. The dialog box lists all existing groups inside DocuSign Signature Appliance and their status (Enabled or Disabled). When a group is Disabled, all users who are members of the group cannot login to DocuSign Signature Appliance.

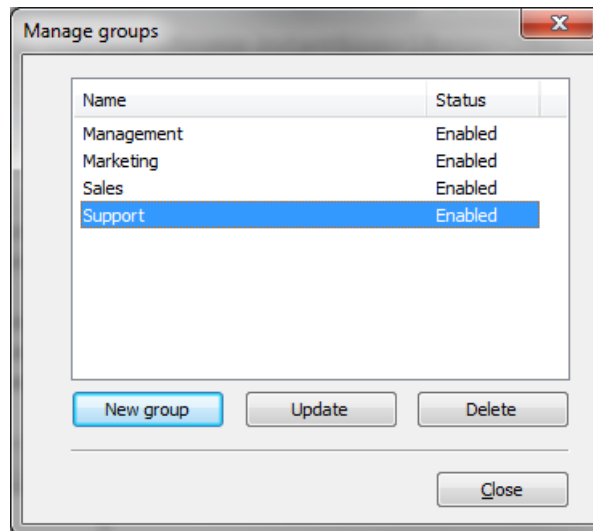


Figure 63 Users Management Utility – Manage Groups Dialog Box

You can perform the following operations:

- **New Group** – Add a new group to DocuSign Signature Appliance. When you click **New Group**, the *Group Settings* dialog box appears:

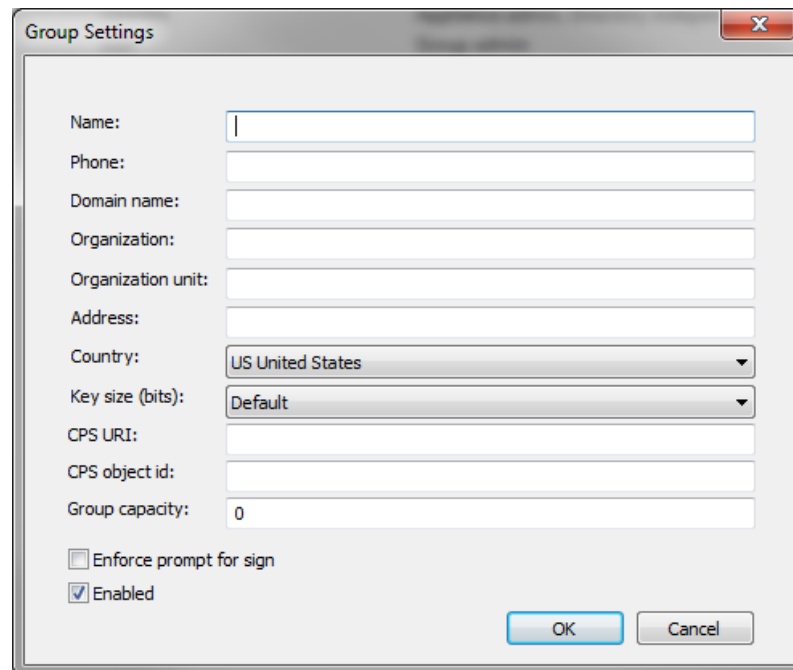


Figure 64 Users Management Utility – Group Settings Dialog Box

You can define the following parameters for a group:

- **Name** – The group name. The name must be unique. This is the only mandatory field in the dialog box.
- **Phone** – A phone number for this group.

- **Domain Name** – The domain name for this group.
- **Organization** – The organization associated with this group. In all certificates of users that belong to this group, the organization parameter will include this Organization value. If this parameter is not empty, then when a user is assigned to a group, the user's certificate is regenerated in order to update it with this parameter value.
- **Organization unit** – A descriptive name for the organizational unit of the group (Sales, Marketing, etc.)
- **Address** – The address of the group.
- **Country** – The country of the group.
- **Key size** – The key size (in bits) of all the users who are group members. If you select **Default**, the key size of group members remains unchanged. However, if you specify a key size, then when a user with a different key size is assigned to the group, that user's key and certificate are regenerated in accordance with the key size you specified.
- **CPS URI** – The Certificate Policy URI for all the users in the group. The certificate of all the users in the group will contain this CPS URI. An empty URI means that the default system CPS URI is used.
- **CPS object ID** – The Certificate Policy object ID for all the users in the group. The certificate of all the users in the group will contain this CPS Object ID. An empty Object ID means that the default system CPS Object ID is used.
- **Group capacity** – The maximum number of users in the group. A value of 0 means that the number of users in the group is not limited and the only restriction is the number of users permitted by the license.
- **Enforce prompt for sign** – If the system parameter **Prompt For Signature** is not selected, you can override the setting, so that each group member is prompted to supply a password before every digital signature operation.
- **Enabled** – Whether the group is Enabled or Disabled. If a group is Disabled, no group member can login to DocuSign Signature Appliance.
- **Update** – Update the selected group. When you click **Update**, the *Group Settings* dialog box appears (Figure 64), displaying the current settings of the group. You can change any of the settings.
- **Delete** – Delete the selected group from the system.
- Double clicking a group in the list displays the *Group Settings* dialog box (Figure 64). You can view and modify any of the settings.

New Group

Note: This operation is not relevant when DocuSign Signature Appliance is deployed in a Common Criteria EAL4+ mode of operation.

Creates a new group. When you select this option, the *Group Settings* dialog box (Figure 64) appears. For explanations, refer to the explanations following (Figure 64).

View Menu

Toolbar

Enables toggling the view of the toolbar.

Status Bar

Enables toggling the view of the status bar.

Filter

Enables the administrator to filter the user display in the main window. When this option is selected, the *Users filter definitions* dialog box appears.

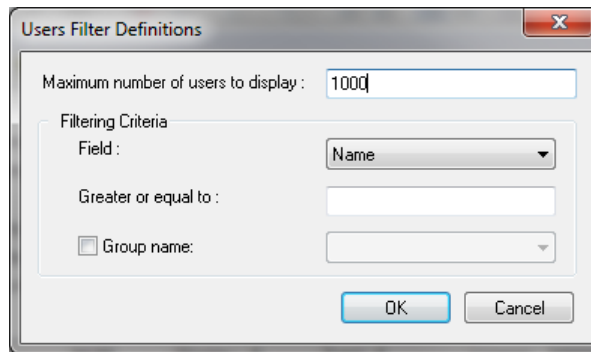


Figure 65 Users Management Utility – Users Filter Definitions Dialog Box

You can filter the users display as follows:

- **Maximum number of users in display** – Set this number to limit the number of users displayed in the main window. Default: 50.
- **Filtering Criteria** – You can specify any of the following filtering criteria:
 - **Field** – Enter a Name, Common Name, or Email,
 - **Greater or equal to** – Enter a string. The greater or equal calculation is based on comparing the string with the value you entered in **Field**.
 - **Group Name** – Check the option and select a group.

The filtering criteria you specify is logically ANDed. Thus for example, if you enter filtering criteria in all three fields, the users list will display only the users belonging to the specified group, whose Name/Common Name/Email is greater than or equal to the given string.

Refresh

Enables re-applying the filter on the users list. The users list refreshes and displays a users list according to the filter criteria.

List Icon Details

Enables defining the display of users in the main window as follows:

- **List** – Only user names are displayed.
- **Icon** – User names are displayed with a big icon.
- **Details** – Each user is displayed together with some user information. Use the **Select Columns** option to specify which information will appear.

Select Columns

When this option is selected, the *Select Columns* dialog box appears. Use the dialog box to define which fields are displayed in the main window when it is defined to display user details.

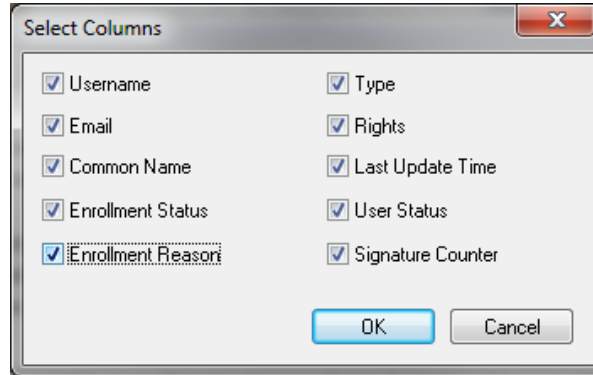












Figure 66 Users Management Utility – Select Columns Dialog Box

Help

Displays the About window that specifies the Users Management version and provides a link to the ARX site.

Users Management Toolbar

The Users Management toolbar contains shortcut buttons to the following options, available also from the drop-down menus:

Button	Task
	Login
	Built-in Login
	Logout
	New User
	Delete User
	Set User Password
	View user properties
	Refresh Users list
	Filter
	About window

Right-click User Menu

To activate the User right-click menu, right-click a user in the main window. The options **Reset user signature counters**, **Reset User Password Counter**, **Delete**, **Set Password**, **Properties** and **Assign Group** (included in **New**) are available also in the **User** drop down menu option of the Users Management utility and are described in [Manage Menu](#). The **Change Status** option is available only through the user's right-click menu. The **Change Status** and **Assign Group** options are described below.

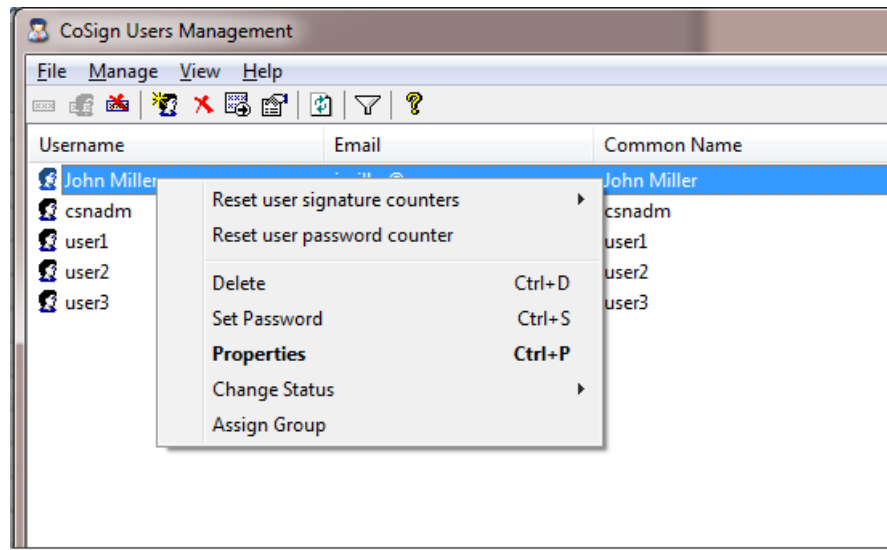


Figure 67 Users Management Utility – Right-click Menu

Change Status

Enables setting the status of a user to either Disabled or Enabled. A Disabled user cannot sign, even if the user belongs to a group that is Enabled. This option is relevant only for a Directory Independent environment.

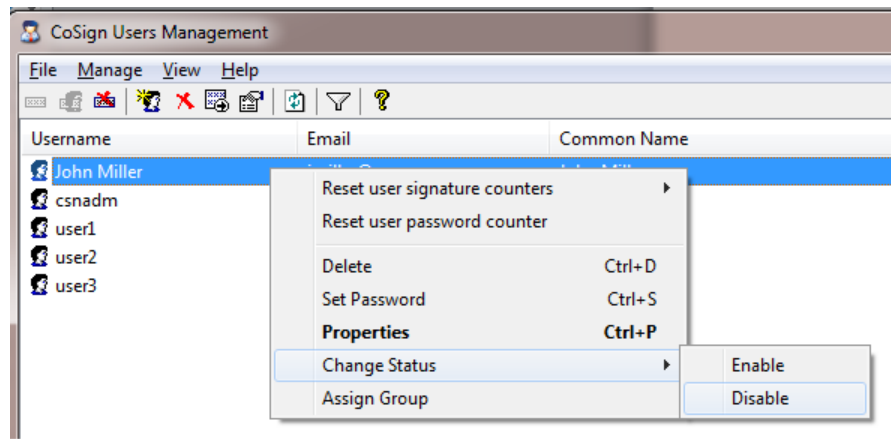


Figure 68 Users Management Utility – Change Status Option

Assign Group

Enables assigning a user to a group, or unassigning a user from a group. When you select this option, the *Manage groups* dialog box appears (Figure 61), with options for assigning/unassigning a user.

Using Command Line Utilities

The following command line utilities can be executed from the administration station, and can be used as part of an overall batch script that is periodically activated:

- GetBackup – Backs up a appliance.
- GetEvt – Retrieves the event log of the appliance.

- `SetSCP` – Sets the working state of the appliance.
- `RestartServer.exe` – Restarts a server.
- `Switch2Prim.exe` – Perform a Switch-to-Prime operation for a given alternate appliance.
- `Groups` – A Windows utility that enables end users to set their current group. This enables the end user to use group keys. This utility cannot be executed in batch mode.

The `GetBackup`, `GetEvt` and `SetSCP` utilities are installed as part of the ARX CoSign Admin component and located under `Program Files\ARX\ARX CoSign Admin Client`. The `Groups` utility is installed as part of the ARX CoSign Client component, and its files are located under `Program Files\ARX\ARX CoSign Client`.

Note: To display the required parameters for a command, execute the command without any parameters.

GetBackup

The `GetBackup` command enables you to back up the DocuSign Signature Appliance to a file located on the local network.

You can have a dedicated machine in the organizational network that can automatically call the `GetBackup` command without specifying a user ID and a password.

Note: This command provides the same functionality as the **All Tasks → Backup** option in the Administration MMC (refer to [Backing up the DocuSign Signature Appliance Data](#)).

The following table describes the available parameters for `GetBackup`:

Parameter	Description
<code>-F <Output File name></code>	Output file name of the backup file.
<code>-IP <IP Address></code>	IP address of the appliance. If this value is omitted, it will be taken from the SCP or from the client configuration.
<code>-A <1, 2, 3, 4></code>	Prompt For Logon value: 1 – SSPI 2 – Server Side Authentication (AD, LDAP) 3 – SSPI User/Password Client (AD) 4 – User Password. Directory Independent If this value is omitted, it will be taken from the SCP or from the client configuration.
<code>-PN <Principal Name></code>	Principal name of the DocuSign Signature Appliance. This is the name of the DocuSign Signature Appliance in the directory service (i.e., csn000001). This parameter is mandatory in Microsoft Active Directory environments. If this value is omitted, it will be taken from the SCP or from the client configuration.
<code>-U <User Name></code>	DocuSign Signature Appliance administrator user name.

Parameter	Description
-P <User Password>	Password of the DocuSign Signature Appliance administrator user.
-D <Domain Name>	Name of the domain or context.

GetEvt

The `GetEvt` command enables you to retrieve an event log from the DocuSign Signature Appliance.

Note: This command provides the same functionality as the **All Tasks → Download Logs → CoSign Event** option in the Administration MMC (refer to [Downloading Log Files](#)).

The following table describes the available parameters for `GetEvt`:

Parameter	Description
-F <Output File name>	Output file name of the event log file.
-IP <IP Address>	IP address of the appliance. If this value is omitted, it will be taken from the SCP or from the client configuration.
-A <1, 2, 3, 4>	Prompt For Logon value: 1 – SSPI 2 – Server Side Authentication (AD, LDAP) 3 – SSPI User/Password Client (AD) 4 – User Password. Directory Independent If this value is omitted, it will be taken from the SCP or from the client configuration.
-PN <Principal Name>	Principal name of the DocuSign Signature Appliance. This is the name of the DocuSign Signature Appliance in the directory service (i.e., csn000001). This parameter is mandatory in Microsoft Active Directory environments. If this value is omitted, it will be taken from the SCP or from the client configuration.
-U <User Name>	DocuSign Signature Appliance administrator user name.
-P <User Password>	Password of the DocuSign Signature Appliance administrator user.
-D <Domain Name>	Name of the domain or context.

restartServer.exe

The `restartServer.exe` utility restarts a server. It has the following syntax:

```
restartServer [-IP <IP address>] -U <User name> -P <Password> [-D <Domain name>] -RK <Restart operation type>
```

The following table describes the available parameters for `RestartServer.exe`:

Parameter	Description
-IP <IP address>	IP address or DNS name of the DocuSign Signature Appliance. This parameter is optional
-U <User name>	User name for authentication based on user name and password.
-P <Password>	Password for authentication based on user name and password.
-D <Domain name>	Domain name for authentication based on user name and password. This parameters is optional.
-RK <Restart operation type>	Type of restart operation: 1 - Reboot the appliance 2 - Shut down the appliance 3 - Restart all services.

Switch2Prim.exe

The Switch2Prim.exe utility performs a Switch-to-Prime operation for a given alternate appliance. It has the following syntax:

```
Switch2Prim.exe -F <File name> [-IP <IP address>] [-A <Authentication kind>] [-PN <Principal name>] [-U <User name>] [-P <Password>] [-D <Domain name>]
```

The following table describes the available parameters for Switch2Prim.exe:

Parameter	Description
-F <File name>	A log file for messages produced as part of the Switch2Prime process
-IP <IP address>	IP address or DNS name of the DocuSign Signature Appliance appliance. This parameter is optional
-A <Authentication kind>	The type of authentication to use when accessing the alternate appliance: 1 – SSPI 2 - Server side authentication 3 - SSPI User Password client side 4 - Push authentication
-PN <Principal name>	The DocuSign Signature Appliance principal name for SSPI authentication. This parameter is optional
-U <User name>	The user name for authentication based on user name and password. This parameter is optional
-P <Password>	The password for authentication based on user name and password. This parameter is optional

Parameter	Description
-D <Domain name>	The domain name for authentication based on user name and password. This parameter is optional

SetSCP

The `SetSCP` command enables you to define in the directory whether the appliance is up or down. This enables or disables the appliance, and thus allows DocuSign Signature Appliance clients to immediately determine whether or not the DocuSign Signature Appliance is active.

Note: In an Active Directory environment you must be joined to the parent domain to activate the SetSCP utility. The utility will not work if the client is joined to the child domain.

Note: This utility is not relevant for a Directory Independent or LDAP environment.

The following table describes the available parameters for `SetSCP`:

Parameter	Description
-D <Domain Name>	Name of the domain or context.
-N <Appliance Name>	Principal name of the DocuSign Signature Appliance appliance. This is the name of the workstation in the directory.
-K <Directory Kind>	Type of directory service. Possible values: A – Microsoft Active Directory.
-S <Working State>	Working state of the DocuSign Signature Appliance appliance. Possible values: Up Down

Groups

`Groups` is a Windows utility that enables end users to set their current group. Any keys and certificates that are created by communicating with an external CA are directed to the specified group.

Note: You must set the Create Group Keys system parameter in order to use group keys. Refer to [Changing System Parameters](#).

Note: This utility is not relevant for a Directory Independent environment since there is no definition of a group in that type of environment.

To set the current group:

- Run the `Groups` utility. The Client Default Group Selection dialog box appears.
- Select a group from the list in the dialog box.
- Click **OK**. Any subsequent enrollment to an external CA (or any other activity that creates keys or certificates) will be directed to this selected group.

Note: All users that belong to this group can use the certificates.

Chapter 6: Using the Consoles

This chapter describes how to connect to and use the consoles to manage DocuSign Signature Appliance. The consoles enable operations that cannot be performed using the Administration MMC.

There are several types of consoles, depending on the DocuSign Signature Appliance hardware type and the DocuSign Signature Appliance hardware version.

Console Types

There are two main types of consoles:

- [Web-based Console](#) for DocuSign Signature Appliance hardware versions 8.0
- [Built-in Console](#) for CoSign hardware versions prior to 8.0

Overview of the Web-based Console for Hardware v8.0

The Central FIPS appliance version 8.0 and Enterprise appliance version 8.0 offer a web-based console as well as a built-in touch screen console. The touch screen console is for display purposes only.

To access the web-based console, you must connect the administrative PC or laptop to the dedicated LAN interface and use a web browser to connect to <http://10.0.0.2/:8088>.

Overview of the Built-in Console for Hardware versions prior to v8.0

For CoSign hardware versions prior to 8.0, a built-in console is provided. Access to the console depends on the appliance type:

- **Built-in Console:** In the FIPS appliance or Central FIPS appliance in a Common Criteria EAL4+ appliance, a built-in console is provided as part of the appliance.
- **Configuring a terminal as a built-in Console:** In the Enterprise appliance, the console functionality is provided by connecting the administrative PC through the serial/USB port and running the console application on the administrative PC. For more information see [Configuring a Terminal as a built-in Console in Hardware versions prior to v8.0](#) and [Using the USB to Serial Adaptor](#).

Configuring a Terminal as a built-in Console in Hardware versions prior to v8.0

Note: This section applies to the Central Enterprise appliance.

In order to use the console, you must first configure the console terminal.

To configure the terminal:

- Start by turning the power switch on.
Note: DocuSign Signature Appliance does not need to be installed at this stage.
- Using the supplied 9-pin crossed serial cable, connect a PC to DocuSign Signature Appliance.
- On the PC, run a terminal emulation application, such as HyperTerminal.

Note: HyperTerminal is supplied as part of the standard Microsoft 2003 installation and can be found under **Start → Programs → Accessories → Communications**.

- Configure the terminal application with the following parameters:
 - **COM port** – The local serial port on the PC to which you connected the cable.
 - **Baud rate (bits per second)** – 9600.
 - **Data bits** – 8.
 - **Parity** – None.
 - **Stop bits** – 1.
 - **Flow Control** – None.
- The main console screen appears on the terminal display. The main console screen displays the main menu.

```

-----
->Status      Reset tamper      Set Time
  Use DHCP    Factory restore  NetWare
  IP addr     Shutdown
  up          down      select
-----
          1          2          3          4
  
```

Figure 69 Main Console Menu

Using the USB to Serial Adaptor

If your PC does not have a serial port, you can use a special USB to Serial adaptor provided with the Central Enterprise package.

To use the adaptor:

- Attach the adaptor to the USB port of your PC and connect the serial side of the adaptor to the DocuSign Signature Appliance.
- When prompted to provide a driver, put the supplied CD into the CDROM drive, and specify the CDROM drive. The PC will find the driver on the CD and install it.
- Configure the terminal application as above. The new adaptor will add a new COM port such as COM3. Use this port as part of the configuration.

Using the Built-in Console –Hardware versions prior to 8.0

The console is constantly running within all DocuSign Signature Appliance models.

- To operate the built-in console in a FIPS appliance, use the four buttons (numbered 1, 2, 3, and 4 from left to right) located on the FIPS appliance's front panel below the display.
- To operate the external console terminal for an Enterprise appliance, use the keyboard keys 1, 2, 3, and 4.

1 and 2 are usually used for moving up and down to locate the desired function, while 3 is usually used for selecting.

Note: The bottom line in the display always shows the current function of each key.

Enterprise refreshes the terminal display every 10 seconds. Therefore, when you first open the console, it may take up to 10 seconds to view the display. To view the display immediately, press any key.

The Central FIPS appliance has a screen saver feature that displays the ARX logo if the console is left idle for more than 10 minutes. Press any button to display the main menu.

The bottom right side of the main menu may contain a flashing message. This indicates a state that requires user intervention. The possible messages are: [TAMPER!], [IP Addr], and [License]. Refer to [Console Problems](#) for more information.

Displaying Status

From the main menu, select `Status`. The DocuSign Signature Appliance information appears (Figure 70). Press 1 and 2 to scroll up and down.

```

-----
|Ser# SIG00201 Mar 24 2008 06:48:26 -0800|
|Version SW4.4 HW4.0 ET 00:16:76:3e:77:27|
|Service Running      Addr 2.3.0.4      |
|                    down      back      refresh|
-----
      1          2          3          4

```

Figure 70 Appliance Information

The following table describes the DocuSign Signature Appliance information parameters:

Parameter	Description
Ser #	The appliance's serial number. This is also the appliance's domain computer name. <i>Note: The FIPS appliance is prefixed CSN, and the Enterprise appliance is prefixed sig.</i>
Date	The current appliance date and time (PDT time zone).
SW Version	The DocuSign Signature Appliance appliance software version.
HW Version	The DocuSign Signature Appliance hardware version.
ET	The Ethernet MAC address of the DocuSign Signature Appliance.
Service	The status of the service. Possible values: Running, Starting, Stopped, Stopping.

Parameter	Description
Install	The installation status of the appliance. Possible values: Installed, Factory, CRP Wait, REPL Wait. Note: If a number is displayed for this parameter, installation is in progress. The number indicates the installation phase.
Addr	IP address of the appliance.
Mask	Subnet mask of the appliance.
GW	IP address of the default gateway.
DNS	IP address of the DNS server.
DNS2	IP address of an alternate DNS server.
DHCP	Indicates whether DHCP is enabled. Possible values: Enabled, Disabled. Disabled means that the IP address should be entered manually. Enabled means that the IP address is taken from the DHCP server.
State	The service state. Possible values: OK, TAMPER!, No IP Address, License Error. Refer to Console Problems in Chapter 9: Troubleshooting for more information.
Link	The network connectivity state. Possible values: 10Mb, 100Mb, 1Gb.
DB size	The size of the database files.
FIPS Mode	Indicates whether the appliance is operating in FIPS mode. Possible values: ON (appliance operating in FIPS mode). Off (appliance not operating in FIPS mode). Note: For DocuSign Signature Appliance to operate in FIPS mode, make sure the following system parameters are set as follows: - Web Services Support is set to False. - Enforce FIPS Approved Algorithms is set to True.
Admin group	The name of the directory users group whose members are allowed to manage DocuSign Signature Appliance via the Administration MMC.
Role	The appliance's role in the High Availability configuration. Possible values: Primary, Alternate, Standalone.
Signers group	Relevant only to Active Directory environment. Indicates the name of the Signers group in Active Directory.

Parameter	Description
WWV Certs (Comodo)	<p>Information that relates to when users' certificates are automatically issued by the Comodo Worldwide verifiable CA.</p> <p>The parameters are displayed in the following format: UUU/VVV Pend W/X, where:</p> <p>UUU is the number of current users in DB.</p> <p>VVV is the maximal number of certificates that can be published for the organization.</p> <p>W is the number of pending certificate requests that were not yet sent to Comodo.</p> <p>X is the number of pending approval certificate requests. These are the certificates requests that were not approved yet by Comodo.</p> <p>Any parameters that are persistently non-zero indicate a problem, such as a networking problem. If the problem persists, contact ARX support at http://www.arx.com/support/supportrequest.</p>
Expired	<p>Displays expiration information.</p> <p>If there is no expiration, the word <i>Infinite</i> is displayed. Otherwise, the expiration date is displayed.</p>

Note: The console's display is **not** automatically refreshed with new data. For example, if the service is in the process of stopping, the **Status** continues to be displayed as **Running**. In order to view updated information, return to the main menu and reselect **Display status**. Use the **Refresh** option to get updated values.

Enabling DHCP

DHCP is enabled by default. If you are currently using a static IP address, you can use this option to switch back to DHCP.

To enable DHCP:

- From the main menu, select **Use DHCP**. The following message appears:

Setting DHCP mode, please wait.

The IP address of the DocuSign Signature Appliance is retrieved from the DHCP server.

- You can view *the* value of the current IP address by selecting **Display status** from the main menu.

Note: The DNS server's address will also be retrieved from the DHCP server after selecting this option.

Using a Static IP Address

To use a static IP address instead of DHCP:

- From the main menu, select **Set IP address**. The current IP address information appears.



Figure 71 IP Address Information

- Enter the IP address, network mask, default gateway, and DNS servers' information. For each parameter, use ← and → (buttons 1 and 2) to move between digits, and use + and - (buttons 3 and 4) to select the desired digit.
- Select **Exit**. When prompted, choose whether to **Save** (button 3) or **Discard** (button 4) the newly set addresses.
- The following message appears when you choose **Save**:

Setting IP address, please wait.

After the IP is set, the following message appears:

DONE

Note: If only the DNS fields are modified, the appliance will continue to use DHCP for getting the IP address, subnet mask, and default gateway address.

Resetting the Tamper Mechanism (Enterprise Only)

If the cover of the Enterprise appliance is opened, the secret key used to protect the database is erased and the power is turned off. The next time DocuSign Signature Appliance is started, the Tamper LED flashes on and off, the Appliance has been tampered with message is displayed, and the flashing [TAMPER!] message is displayed in the main menu. The tamper mechanism must be reset before DocuSign Signature Appliance can be used.

To reset the tamper mechanism:

- From the main menu, select **Reset tamper**.
- At the prompt, insert one of the backup MiniKey tokens. The following message appears:

Please insert a backup Minikey that was created during installation

- After the backup MiniKey is inserted, the following message appears:

**Resetting tamper, please wait ...
Done.**

- Remove the backup MiniKey token and insert the license MiniKey token.

Note: If you insert the incorrect backup MiniKey token, the *Failed, press any key to continue* message is displayed and the tamper LED continues to flash. Perform the procedure again using the correct backup MiniKey token.

Note: It is recommended to activate the Sync with Directory option after resetting the tamper mechanism. For more information, refer to [Synchronizing DocuSign Signature Appliance with the Directory Service](#).

Restoring Factory Settings

The console enables you to restore DocuSign Signature Appliance to its factory settings. You may want to do this in any of the following circumstances:

- DocuSign Signature Appliance was installed for demo, pilot, or development purposes, and you now want to reinstall the DocuSign Signature Appliance software for production purposes.
- You want to reinstall the DocuSign Signature Appliance software with different parameters.
- Installation failed or was stopped, and the DocuSign Signature Appliance software cannot be reinstalled again without restoring factory settings.

Restoring factory settings performs the following functions:

- Deletes all data from the database, including all users, keys, and certificates.
- Uninstalls the CA located within DocuSign Signature Appliance.
- Unregisters DocuSign Signature Appliance from the domain.
- Resets all DocuSign Signature Appliance installation parameters to the default values.
- Resets the DocuSign Signature Appliance.

Note: In Active Directory environments, unregistering the DocuSign Signature Appliance removes the appliance from the domain, but does not remove the computer from the Active Directory. To fully unregister the Appliance, manually remove the computer from the Active Directory.

Note: If the DocuSign Signature Appliance was configured to receive certificates from a WWV external CA automatically, the operator will be asked whether to revoke the existing certificates in the external CA.

You may want to keep the existing certificates if you are intending to perform a restoration operation right after the Reset to factory settings operation. If you choose to keep existing certificates, old certificates will not be revoked and the user can continue using the existing certificates.

To restore factory settings:

- From the main menu, select **Factory restore**.
- Enter **yes** to confirm the operation.

Shutting Down

To shut down CoSign:

- From the main menu, select **Shutdown**.
- Enter **yes** to confirm the operation.

Setting Time

This option enables the operator to update the CoSign clock. This parameter is very important since it affects the effective start date of a user certificate generated by CoSign, as well as affecting Active Directory user authentication.

You can modify the CoSign time by either modifying the contents of CoSign's date and time fields, or by specifying that CoSign time will be constantly updated by the time of an NTP server.

To set the CoSign time:

- From the main menu, select **Set Time**.

The current time is displayed.

```

-----
|Date Sep 01 2004   Time 12:59:00 -0800 |
|NTP Server 000.000.000.000                |
|                                     Exit |
|  <-           ->           +           - |
|   1             2             3             4 |
-----

```

Figure 72 Setting CoSign Time

- To modify the date and time fields, use the arrows to specify the field you wish to modify. Use the + and – buttons to modify the content of the field. Repeat for every field you wish to modify.
- Alternatively, you can specify an NTP server IP address. This option constantly updates the CoSign Server time according to the NTP server time.

Notes:

If you modify the Date or Time fields, any value entered in the NTP server field is ignored and set to all zeros.

If you wish to stop being updated by the NTP server, change the NTP Server field to all zeros.

By default, in an Active Directory environment, the clock is automatically synchronized with a Domain Controller. In this case, the text “AD Sync” will appear next to the NTP Server field.

The time zone offset (“-0800” in [Figure 72](#)) cannot be updated and is displayed for informational purposes only.

- Use the arrows to navigate to **Exit**. When prompted, choose whether to **Save** (button 3) or **Discard** (button 4) the new settings.

Re-synchronizing with Active Directory

If you modify the time, synchronization with Active Directory is lost. To re-synchronize with Active Directory:

- Change the NTP server address from 0.0.0.0 to 10.0.0.1 (that is, not a real NTP server) and press **Save**.
- Change the NTP server address from 10.0.0.1 back to 0.0.0.0 and press **Save** again.

CoSign is now synchronized with Active Directory.

Using the Web-based Console

Starting from DocuSign Signature Appliance hardware version 8, both the FIPS model and the Enterprise model have a web-based console.

To access the web-based console, the appliance administrator must connect a PC or laptop to the dedicated LAN interface, and use a web browser to connect to <http://10.0.0.2:8088>.

The main window appears.

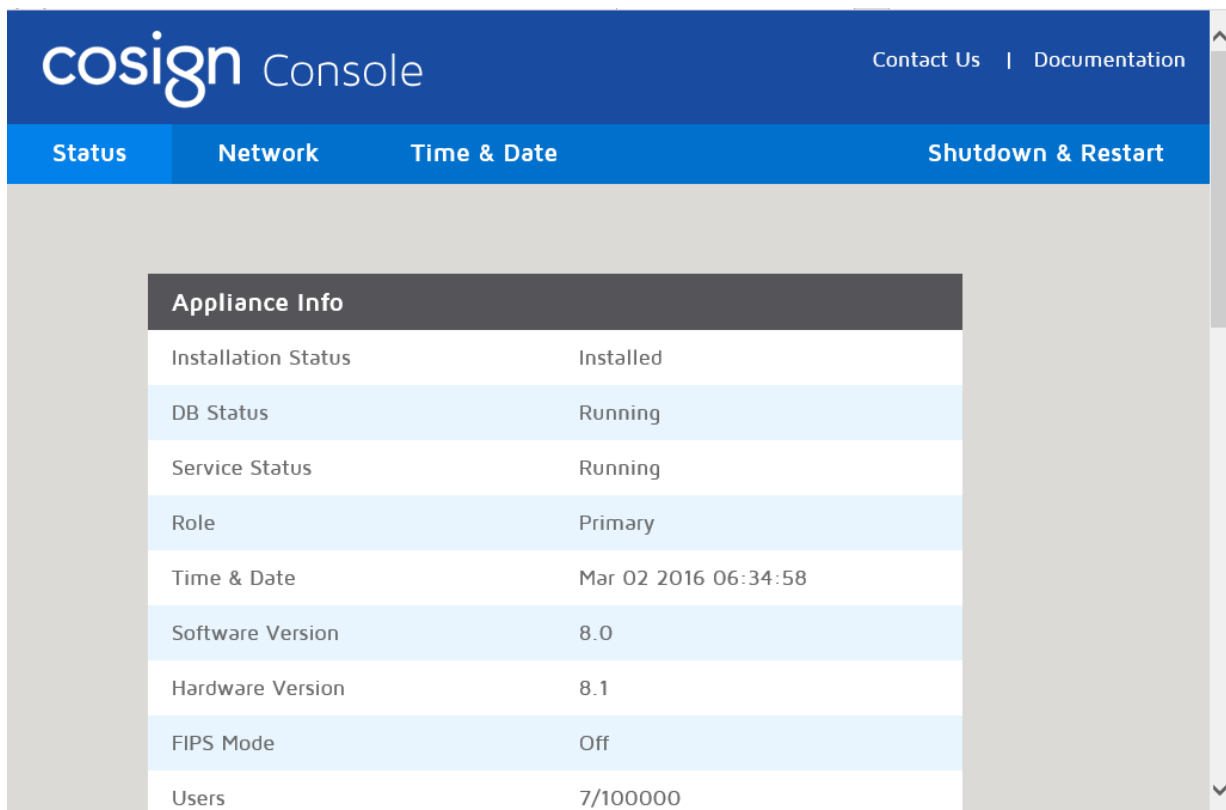


Figure 73 Web-based Console – Main Window

The functionality of the web-based console is very similar to the functionality offered by the built-in console. You can either view information (such as the IP address of the appliance) or perform an administrative action such as setting the IP address of the appliance.

Whenever an action is performed, the administrator is required to:

- Confirm the action. This results in appliance shutdown.

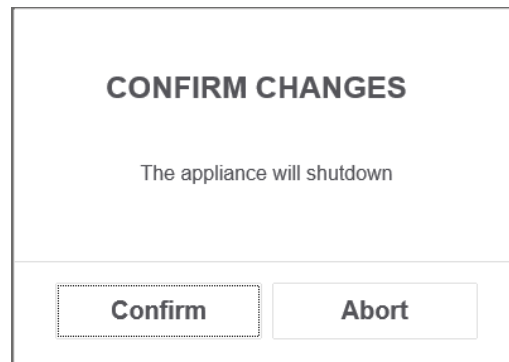


Figure 74 Web-based Console – Confirm Changes

- Commit the changes by removing and re-inserting the license token in order to prove physical access to the appliance.

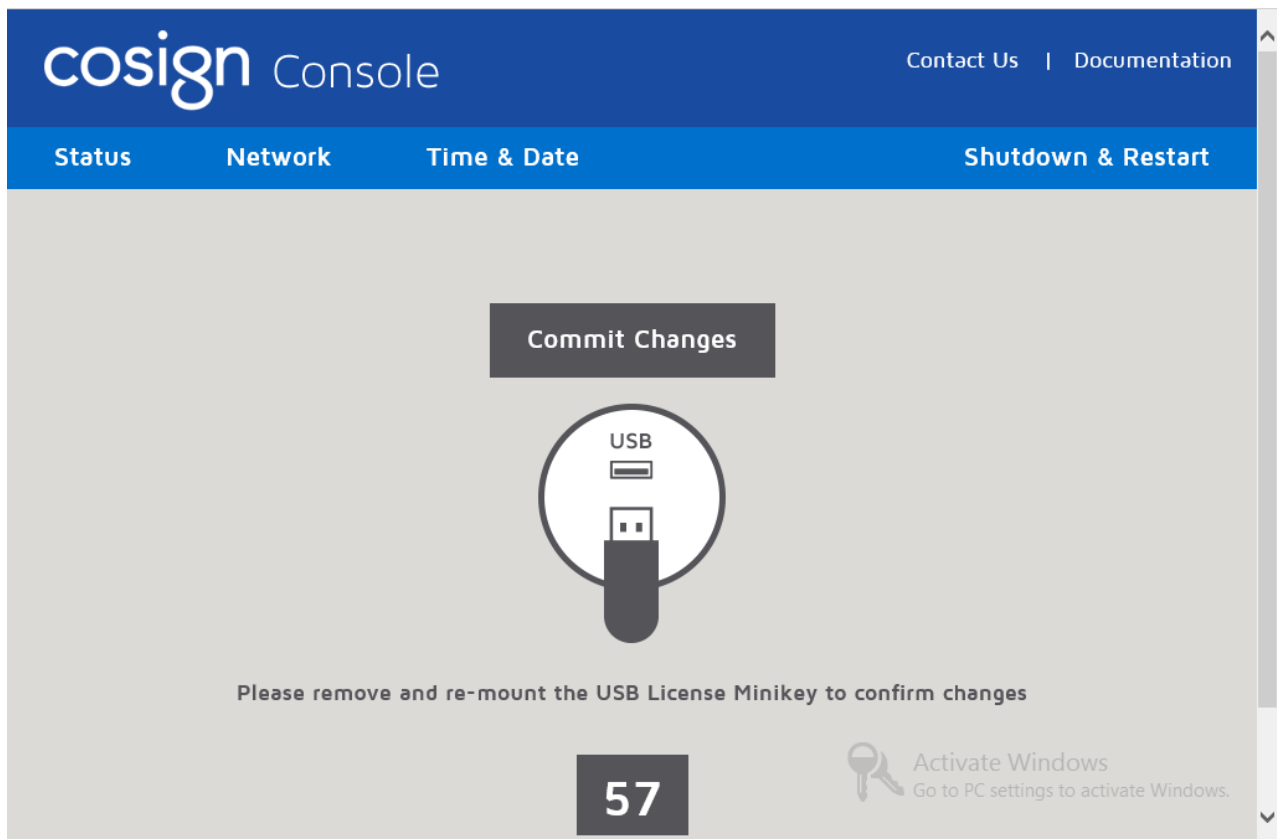


Figure 75 Web-based Console – Commit Changes

Setting the Appliance IP Address

To set the CoSign IP address:

- In the main window, select the **Network** tab.

The screenshot shows the 'Network Settings' section of the web-based console. It is divided into two main sections: 'DHCP' and 'IP Address'. The 'DHCP' section has a radio button selected and two checkboxes for 'IPv4' and 'IPv6'. The 'IP Address' section has a radio button unselected and several input fields: 'IP Address', 'IP Mask', 'IP GW', 'DNS IP', and 'DNS2 IP'. To the right of these fields are 'Subnet Prefix Length' (set to 0) and 'IP GW'. At the bottom, there are two read-only fields: 'MAC' (00:1e:67:e6:d2:68) and 'Link (speed)' (1GB). The interface has a blue header with tabs for 'Status', 'Network', 'Time & Date', and 'Shutdown & Restart'.

Figure 76 Web-based Console – Network tab

- Specify whether the address will be supplied in **IPv4** or **IPv6** format.
- Specify one of the following:
 - **DHCP** - The system will use **DHCP** to obtain the IP address, network mask, default gateway, and DNS servers' information. If you select DHCP you cannot manually enter any of the information.
 - **IP Address** – The system will use the information you enter manually. Enter the IP address, network mask, default gateway, and DNS servers' information

Note that only the operational LAN interface IP address can be updated. The administrative LAN interface is the fixed IP address of 10.0.0.2.

Setting Time

This option enables the operator to update the DocuSign Signature Appliance clock. This parameter is very important since it affects the effective start date of a user certificate generated by DocuSign Signature Appliance, as well as affecting Active Directory user authentication.

You can modify the time by either modifying the contents of DocuSign Signature Appliance's date and time fields, or by specifying that time will be constantly updated by the time of an NTP server.

To set the time:

- In the main window, select the **Time & Date** tab.

The current time is displayed.

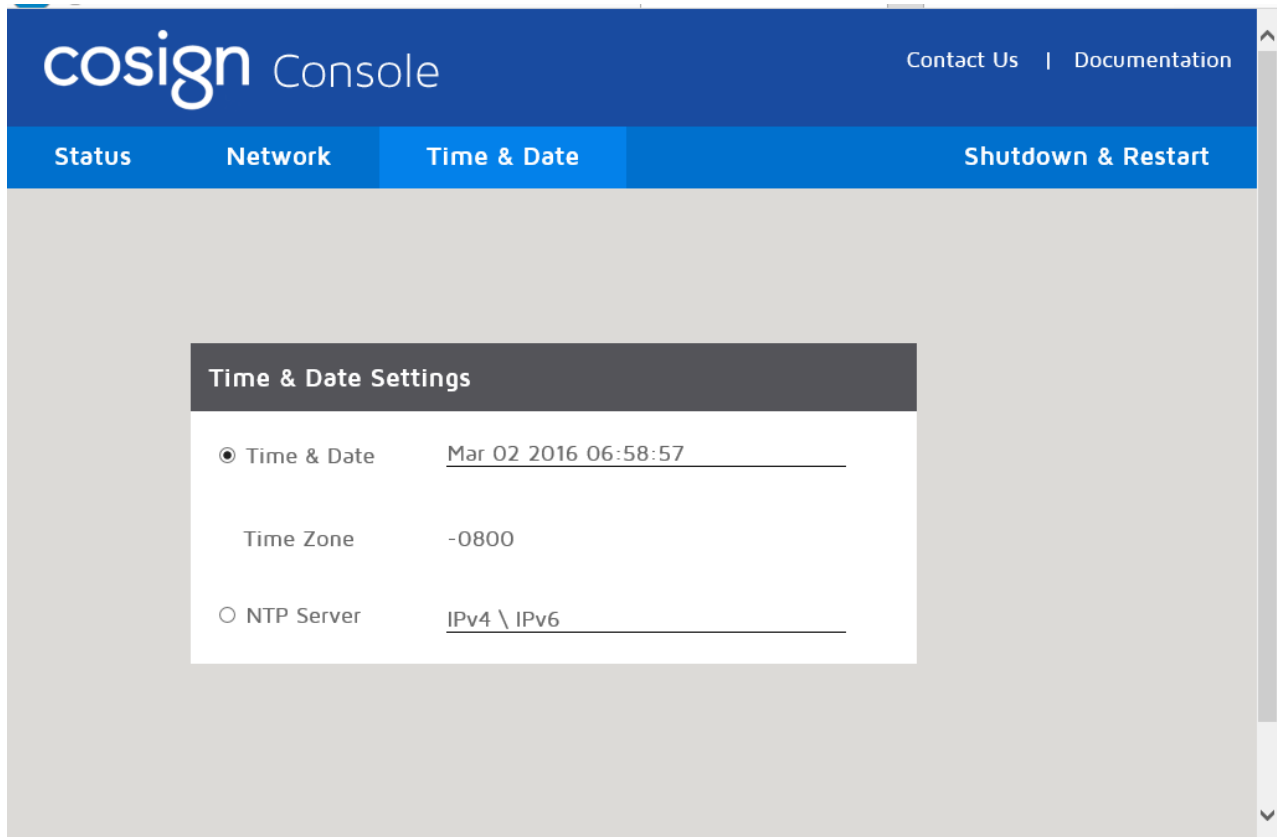


Figure 77 Web-based Console – Time & Date tab

- To modify the date and time fields, select **Time & Date** and modify the values in the following window that appears.

Note that the time zone offset of -0800 (i.e., Pacific Time zone) cannot be updated and is displayed for informational purposes only.

Figure 78 Setting Time

Alternatively, you can specify an **NTP server** IP address. This option constantly updates the server time according to the NTP server time. The NTP server IP address can be specified in either **IPv4** or **IPv6** format.

Shutting Down

To shut down DocuSign Signature Appliance:

- In the main window, select the **Shutdown & Restart** tab.

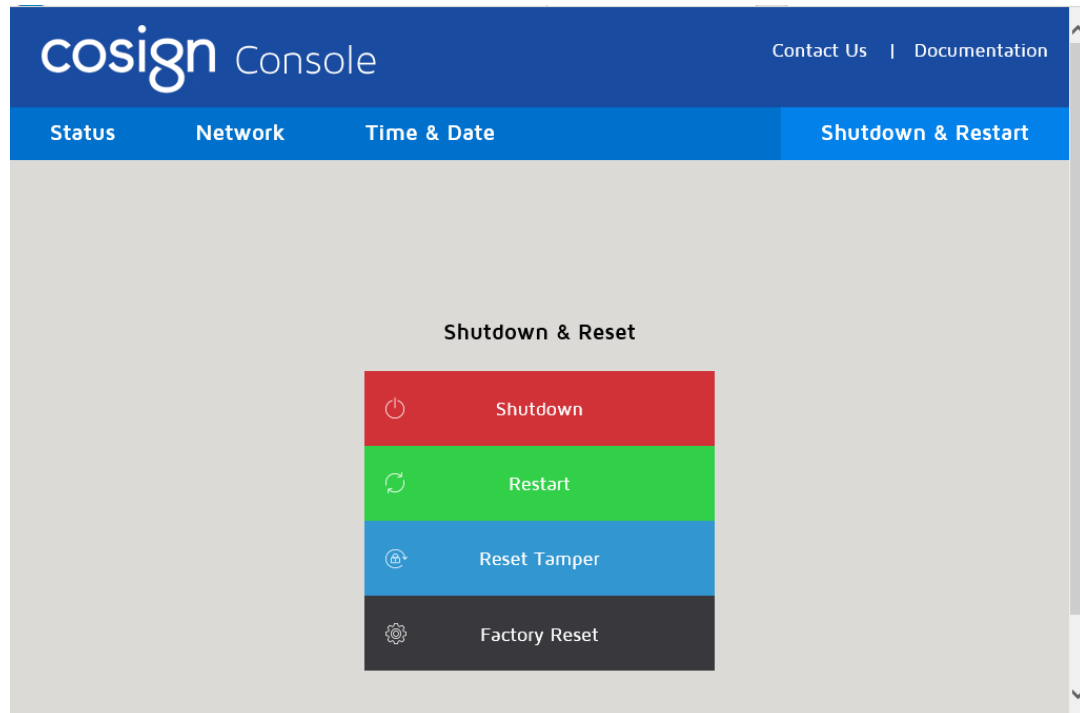


Figure 79 Web-based Console – Shutdown & Restart tab

- In the Shutdown & Reset menu, select **Shutdown**.
- Enter **yes** to confirm the operation.

Restarting the Appliance

To restart the appliance:

- In the main window, select the **Shutdown & Restart** tab (Figure 79).
- In the Shutdown & Reset menu, select **Restart**.
- Enter **yes** to confirm the operation.

Resetting the Tamper Mechanism

To reset the tamper mechanism:

- In the main window, select the **Shutdown & Restart** tab (Figure 79).

- In the Shutdown & Reset menu, select **Reset tamper**.
- At the prompt, insert one of the backup MiniKey tokens. The following message appears:

```
Please insert a backup Minikey that was created during
installation
```
- After the backup MiniKey is inserted, the following message appears:

```
Resetting tamper, please wait ...
Done.
```
- Remove the backup MiniKey token and insert the license MiniKey token.

Note: If you insert the incorrect backup MiniKey token, the *Failed, press any key to continue* message is displayed and the tamper LED continues to flash. Perform the procedure again using the correct backup MiniKey token.

Note: It is recommended to activate the Sync with Directory option after resetting the tamper mechanism. For more information, refer to [Synchronizing DocuSign Signature Appliance with the Directory Service](#).

Restoring Factory Settings

The console enables you to restore DocuSign Signature Appliance to its factory settings. You may want to do this in any of the following circumstances:

- DocuSign Signature Appliance was installed for demo, pilot, or development purposes, and you now want to reinstall the DocuSign Signature Appliance software for production purposes.
- You want to reinstall the DocuSign Signature Appliance software with different parameters.
- Installation failed or was stopped, and the DocuSign Signature Appliance software cannot be reinstalled again without restoring factory settings.

Restoring factory settings performs the following functions:

- Deletes all data from the database, including all users, keys, and certificates.
- Uninstalls the CA located within DocuSign Signature Appliance.
- Unregisters DocuSign Signature Appliance from the domain.
- Resets all DocuSign Signature Appliance installation parameters to the default values.
- Resets the DocuSign Signature Appliance.

Note: In Active Directory environments, unregistering the DocuSign Signature Appliance removes the appliance from the domain, but does not remove the computer from the Active Directory. To fully unregister the DocuSign Signature Appliance, manually remove the computer from the Active Directory.

Note: If the DocuSign Signature Appliance was configured to receive certificates from a WWV external CA automatically, the operator will be asked whether to revoke the existing certificates in the external CA.

You may want to keep the existing certificates if you are intending to perform a restoration operation

right after the Reset to factory settings operation. If you choose to keep existing certificates, old certificates will not be revoked and the user can continue using the existing certificates.

To restore factory settings:

- In the main window, select the **Shutdown & Restart** tab (Figure 79).
- In the Shutdown & Reset menu, select **Factory Reset**.
- Enter **yes** to confirm the operation.

Displaying Appliance Status**To display appliance status:**

- In the main window, select the **Status** tab.

cosign Console Contact Us | Documentation

Status | Network | Time & Date | Shutdown & Restart

Appliance Info	
Installation Status	Installed
DB Status	Running
Service Status	Running
Role	Primary
Time & Date	Mar 02 2016 06:34:58
Software Version	8.0
Hardware Version	8.1
FIPS Mode	Off
Users	7/100000
Transactions	0/Unlimited
License expiration date	Infinite
DB Size	19MB
Admin Group Name	Administrators
Serial Number	SIG02909

Networking	
IP Address	212.25.66.155
IP Mask	255.255.255.0
IP GW	212.25.66.1
DNS IP	212.25.66.7
DNS2 IP	212.25.66.11
IPv6 Address	
Link Local IPv6	fe80::79e7:99f3:e77c:1aab
Subnet Prefix Length	0
IPv6 GW	
DNS IPv6	
DNS2 IPv6	
DHCP	True
MAC	00:1e:67:e6:d2:68
Link (speed)	1GB

Figure 80 Web-based Console – Status tab

The following table describes the appliance status information parameters:

Parameter	Description
Installation Status	The installation status of the appliance. Possible values: Installed, Factory, CRP Wait, REPL Wait. Note: If a number is displayed for this parameter, installation is in progress. The number indicates the installation phase.
DB Status	The status of the database. Possible values: Running, Starting, Stopped, Stopping.
Service Status	The status of the service. Possible values: Running, Starting, Stopped, Stopping.
Role	The appliance's role in the High Availability configuration. Possible values: Primary, Alternate, Standalone.
Time & Date	The current appliance date and time (PDT time zone).
Software Version	The appliance software version.
Hardware Version	The appliance hardware version.
FIPS Mode	Indicates whether the appliance is operating in FIPS mode. Possible values: ON (appliance operating in FIPS mode). Off (appliance not operating in FIPS mode). Note: For DocuSign Signature Appliance to operate in FIPS mode, make sure the following system parameters are set as follows: - Web Services Support is set to False. - Enforce FIPS Approved Algorithms is set to True.
Users	The amount of actual users in the database and the maximum amount of users in the license.
Transactions	The number of actual transactions performed so far and the maximum number of transaction allowed by the license.
License expiration date	Displays expiration information. If there is no expiration, the word <i>Infinite</i> is displayed. Otherwise, the expiration date is displayed.
DB size	The size of the database files.
Admin group Name	The name of the directory users group whose members are allowed to manage DocuSign Signature Appliance via the Administration MMC.
Serial Number	The serial number of the appliance.
IP Address	IP address of the appliance, in IPv4 format.
IP Mask	Subnet mask of the appliance, in IPv4 format.
IP GW	IP address of the default gateway, in IPv4 format.
DNS IP	IP address of the DNS server, in IPv4 format.
DNS2 IP	IP address of an alternate DNS server, in IPv4 format.
IPv6 Address	IPv6-related information.

Parameter	Description
Link Local IPv6	IPv6-related information.
Subnet Prefix Length	IPv6-related information
IPv6 GW	IPv6-related information.
DNS IPv6	IPv6-related information.
DNS2 IPv6	IPv6-related information.
DHCP	Indicates whether DHCP is enabled. Possible values: Enabled, Disabled. Disabled means that the IP address should be entered manually. Enabled means that the IP address is taken from the DHCP server.
MAC	The Ethernet MAC address of the appliance.
Link (speed)	The network connectivity state. Possible values: 10Mb, 100Mb, 1Gb.

Using the Touch Screen of a DocuSign Signature v8.0 Appliance

The touch screen of the DocuSign Signature Appliance shows the main appliance status information. The touch screen is view only, and no operations can be performed.



cosign	
Serial Number	SIG02909 - Primary
Critical Alerts	Off
Installation Status	Installed
Service Status	Running
Version	SW: 8.0 HW: 8.1
IP Address	212.25.66.155
IPv6 Address	

Figure 81 Appliance Touch Screen

Errors such as tamper or license problems are displayed in the **Critical Alerts** line.

Restoring the Appliance After an Internal Hard Disk Failure

In CoSign Hardware V7.0

The appliance provides a mechanism for full appliance recovery and return to factory settings in a case where there is a critical failure in the internal hard disk that prevents the software from booting and running normally.

This option should be used only if the console does not reach the regular operating Menu and instead displays *CoSign is now starting, please wait*, or displays no message at all even though the appliance is powered.

Note: It is highly recommended to consult with ARX technical support before performing a comprehensive factory restore.

To perform a comprehensive factory restore:

- Restart the appliance.
- When the appliance starts, the following message appears for two seconds:
Press the service key to enter the service console.
- Press button 1.
The Service menu is activated.
- A *please select* message appears, prompting you to select between **Quit** and **Restore**.
- Select **Restore**.

Note: If you select **Quit**, the appliance continues to boot in the normal fashion.

A final caution message appears: **Restoring will erase all existing data. Are you sure?**

- Select **Yes**.

Note: If you select **No**, the appliance continues to boot in the normal fashion.

The Comprehensive Restore operation begins. The entire content of the firmware, including the data, is restored using a disk image that was created by ARX during manufacturing.

You can now perform a restore operation using an existing backup file, or perform a new installation.

In DocuSign Signature Appliance Hardware V8.0

The appliance provides a mechanism for full appliance recovery and return to factory settings in a case where there is a critical failure in the internal hard disk that prevents the software from booting and running normally.

This option should be used only if the console does not reach the regular operating Menu and instead displays *CoSign is now starting, please wait*, or displays no message at all even though the appliance is powered.

Note: It is highly recommended to consult with ARX technical support before performing a comprehensive factory restore.

To perform a comprehensive factory restore:

- Restart the appliance and connect a keyboard to the USB port.
In the case of a Enterprise appliance, connect a monitor as well.
- When the appliance starts, the following message appears for two seconds:
Press S to start the service console.
- Press the **S** keyboard key.
The Service menu is activated.

- A *please select* message appears, prompting you to select between **quit(Q)** and **restore(R)**.
- Select **Restore**.

Note: If you select **quit(Q)**, the appliance continues to boot in the normal fashion.

A final caution message appears: **Restoring will erase all existing data. Are you sure Y/N?**

- Select **Yes(Y)**.

Note: If you select **No(N)**, the appliance continues to boot in the normal fashion.

The Comprehensive Restore operation begins. The entire content of the firmware, including the data, is restored using a disk image that was created by ARX during manufacturing.

You can now perform a restore operation using an existing backup file, or perform a new installation.

Chapter 7: Configuring High Availability

The high availability configuration enables an organization to setup several appliances to provide the following:

- *Redundancy* – If an appliance is not available, the other appliances in the network continue to provide the essential digital signature functionality to the client.
- *Load Balancing* – When the organization requires large volumes of digital signature operations, several appliances can be used in parallel to improve performance.

This chapter provides an overview of the high availability configuration, followed by a detailed description of how to set up the system for high availability functionality.

Overview of High Availability

To enable a high availability site, several DocuSign Signature Appliances are installed. All the DocuSign Signature Appliances are connected to the organizational network and are provided with either static IP address or dynamic IP address. One of the DocuSign Signature Appliances is defined as the *primary appliance*, and the other appliances in the site are defined as *alternate appliances*. The group consisting of the primary appliance and the alternate appliances is referred to as a *high availability cluster*. Information is replicated securely from the primary to the alternate appliances.

The primary DocuSign Signature Appliance:

- Contains the internal CA, and serves as the master database of the DocuSign Signature Appliances site.
- Performs all administrative operations such as synchronizing with the Directory's users database and generating keys and certificates for all the relevant users.
- When using an external automatic Worldwide verifiable CA, the primary DocuSign Signature Appliance communicates with the Worldwide verifiable CA to obtain end user certificates.

The administrative operations can only be performed in the primary appliance, therefore if the primary appliance is down, none of these operations can be performed until the primary appliance is up again

Note: Even in high availability configuration, you still need to periodically perform a backup of the primary appliance (using the Administration MMC or the `GetBackup` utility), in order to be able to re-install the primary appliance if it fails.

An **alternate DocuSign Signature Appliance** is more limited in operations compared to the primary DocuSign Signature Appliance, but it provides all digital signature operations. Thus it can provide the necessary Redundancy requirement if the primary DocuSign Signature Appliance is not available, and the necessary Load Balancing requirement for large volumes of digital signature operations.

Information Replication: To enable proper operation of the alternate DocuSign Signature Appliances, the information that exists inside the primary DocuSign Signature Appliance is replicated to the alternate appliances. The replication is performed through the network using secure mechanisms, which disable eavesdropping on the secret data transferred between the primary appliance and the alternate appliances.

By default, the replication occurs every minute and sends all changes that occurred during the last minute. If a replication attempt fails, retries occur in one-minute intervals. The replication process stops after 10 failed retry attempts.

Note: During information replication, data is transferred using the standard IPSEC protocol, with authentication based on a shared secret. The shared secret is based on a key that is diversified from the Server Master Key that is located in the Backup MiniKey.

Client behavior in a high availability configuration:

In a high availability configuration, the client retrieves the IP addresses of all the DocuSign Signature Appliances from the SCP (in Active Directory and NDS environments), or from the local machine setting (in LDAP and Directory Independent environments). It then randomly selects an available DocuSign Signature Appliance when a digital signature operation is required.

For information about the SCP, refer to [Distributing DocuSign Signature Appliance Information through the SCP](#).

For information about configuring the appliance in the client settings, refer to the Client – Appliances section in the *Configuration Utility* chapter of the *DocuSign Signature Appliance User Guide*.

However, when running an administrative client that performs administrative tasks such as inserting a new user to the system, the client will only use the primary DocuSign Signature Appliance.

Installing Appliances in a High Availability Configuration

In a high availability configuration, the order of installation is as follows:

- Install the primary appliance.
- Install the alternate appliances.

The following sections describe the installation process.

Installing the Primary DocuSign Signature Appliance

Installing a primary appliance is identical to installing a stand-alone appliance (refer to [Installing the CoSign Appliance Hardware version 7.0](#), [Installing the DocuSign Signature Appliance Hardware version 8.0](#) and [Installing the Appliance Software](#)). During software installation, the administrator specifies the user management environment (i.e., Active Directory or Directory Independent).

Installing an Alternate DocuSign Signature Appliance

The following sections describe the hardware and software installation of an alternate appliance.

Installing the Alternate Appliance Hardware

Prepare the alternate DocuSign Signature Appliance for installation, and perform the hardware installation of the appliance, as described in [Installing the CoSign Appliance Hardware version 7.0](#) and [Installing the DocuSign Signature Appliance Hardware version 8.0](#).

Installing the Alternate Appliance Software

Note: For proper installation of an alternate DocuSign Signature Appliance in an Active Directory environment, you must have the same permissions as the installer of the primary DocuSign Signature

Appliance. Refer to [Installing DocuSign Signature Appliance in a Microsoft Active Directory Environment](#).

To install the alternate appliance software:

- Open the Control Panel as follows: Open the **Start** menu and select **Programs** → **ARX CoSign** → **CoSign Control Panel**. The Control Panel appears.
- Click the CoSign **Appliances Management** icon. The ARX CoSign Appliance Management window appears.
- Login to the appliance using either the built-in administrator or another admin account.
- Right-click the primary appliance, select **All Tasks**, and then select **High Availability** → **Install Alternate**.
- The *Network setup* dialog box appears.

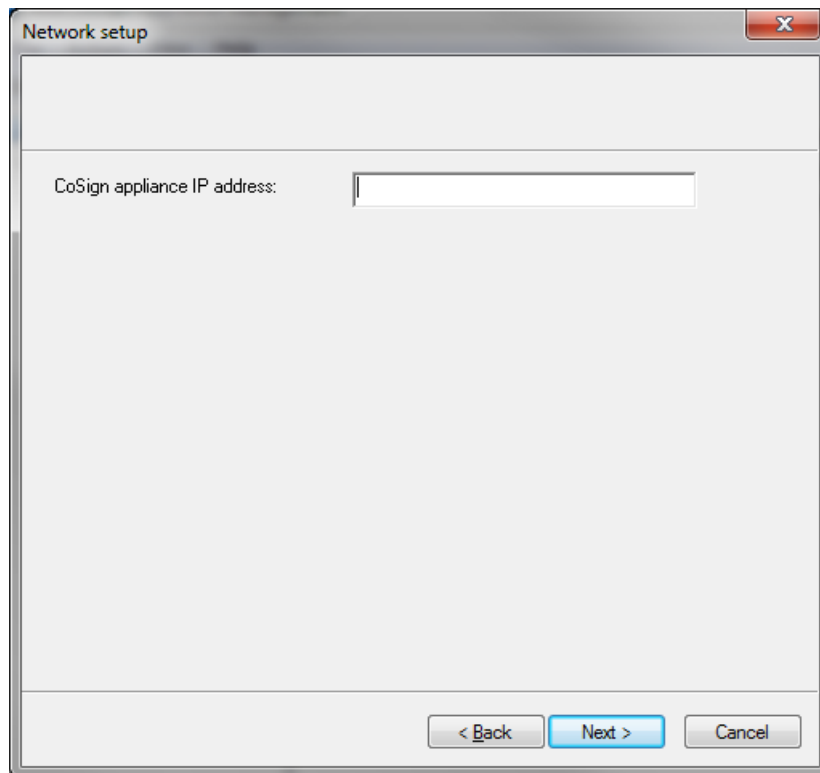


Figure 82 Network Setup Dialog Box

Enter the IP address of the alternate appliance. This parameter is necessary for enabling basic communication to and from the appliance.

Note: For information on setting up the IP address of the appliance, refer to [Using a Static IP Address](#) and [Enabling DHCP](#).

It is highly recommended to use a static IP address for the alternate appliances. If a dynamic (DHCP based) address is used, and the appliance's address changes after the installation, the replication process will fail and a manual re-initialization will be required.

- In the case of an Active Directory installation, enter the user name and password of an administrative account with permission to join the alternate appliance to the domain.

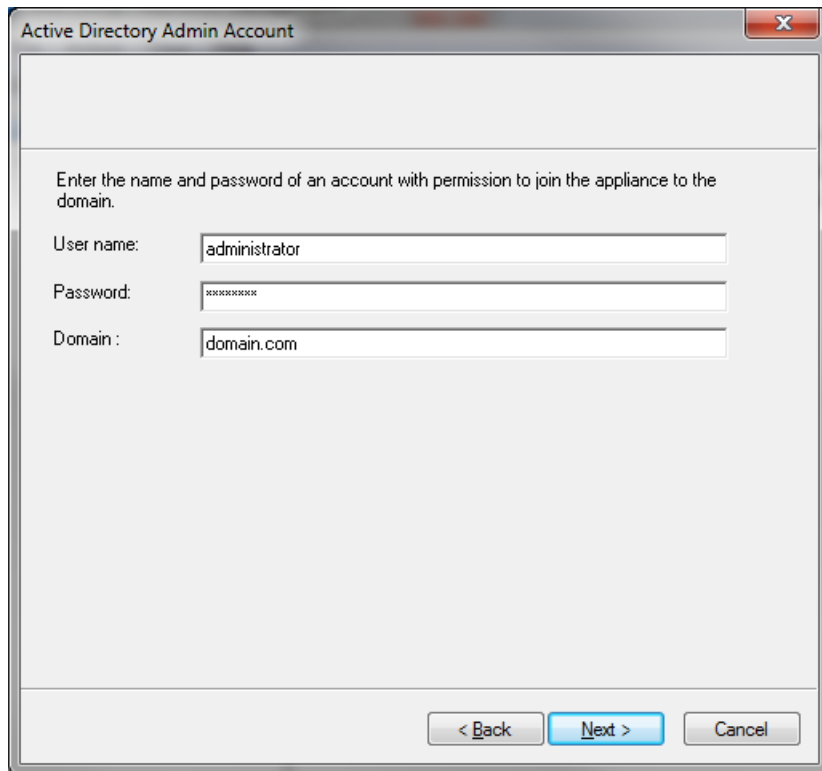
The image shows a Windows-style dialog box titled "Active Directory Admin Account". It contains a text area with the instruction: "Enter the name and password of an account with permission to join the appliance to the domain." Below this are three input fields: "User name:" with the text "administrator", "Password:" with masked characters "XXXXXXXXXX", and "Domain:" with the text "domain.com". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Figure 83 Active Directory Admin Account Dialog Box

- Click **Next**. installation begins. A status bar displays the status of the installation operation.

During the installation, status messages appear on both the console display and the Administration MMC display.

At the **Please insert a backup Minikey** prompt, insert one of the backup MiniKey tokens that were created during the installation of the primary appliance.

It is very important to insert the correct backup MiniKey token since the token contains a set of Triple-DES Master Key of the primary Device, which are used to decrypt the keys database and check the integrity of the users database.

Inserting an improper key will lead to improper authentication of the communication between the primary appliance and the alternate appliance, which will cause the replication to fail.

- At the **Please insert your License Minikey** prompt, insert the license MiniKey token.

Take care to insert the license MiniKey that is dedicated to this alternate appliance. For example, if four appliances are installed in the same site, each of the appliances should have its own license MiniKey, which means there will be four license MiniKeys in the site.

The progress bar continues to display the progress of the operation. The primary appliance database is copied over the network to the alternate appliance.

- At the end of the installation, the following message appears:

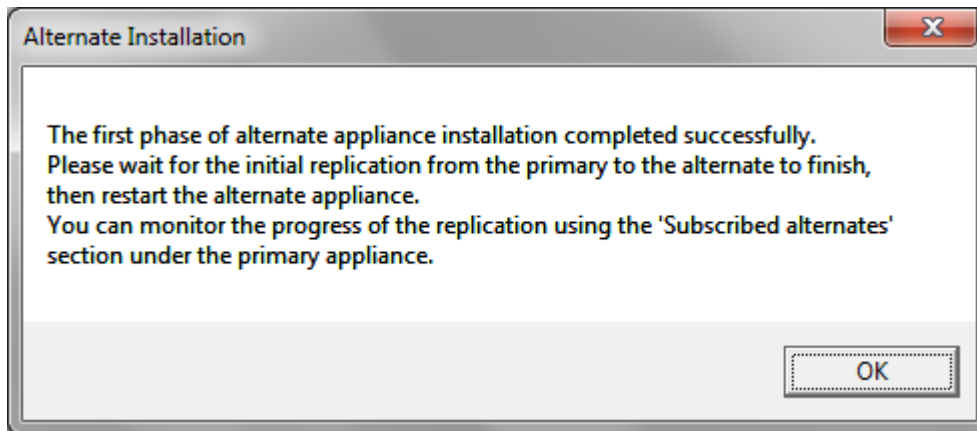


Figure 84 Initial Replication Message

Data replication between the primary appliance and the alternate appliance continues after alternate installation ends.

- Click **OK**.

Note: If the first stage of installation was unsuccessful, the appliance returns to its factory settings. This enables you to rerun the installation. In this case, the status bar displays that installation was unsuccessful, and you can click the **Back** buttons to modify settings before rerunning the installation.

If the installation was unsuccessful and you are unable to rerun the installation, restore an appliance to factory settings and then try again. For more information about restoring factory settings, refer to [Restoring Factory Settings](#).

- In the *ARX CoSign Appliance Management* window, right-click **CoSign appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed alternate appliance.

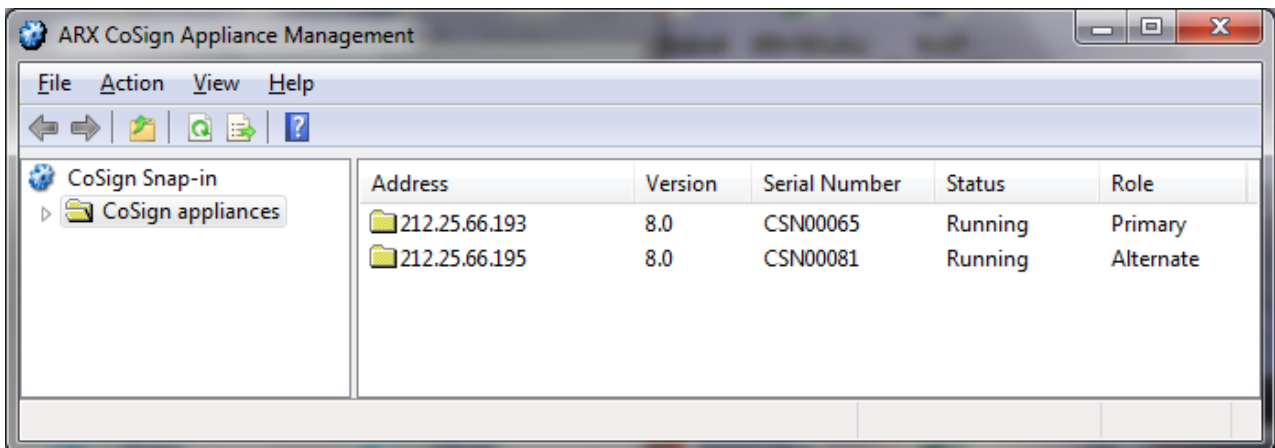


Figure 85 ARX CoSign Appliance Management Window – Displaying Primary and Alternate Appliances

- Verify that all data was indeed replicated to the alternate appliance (refer to [Managing Data Replication in the Alternate Appliance](#)). The replication state should be OK (refer to [Viewing Replication Status of an Alternate Appliance](#)).

- Perform a hard restart of the alternate appliance. The restart ensures that the alternate appliance starts using replicated data, such as system parameters; otherwise, unexpected results may occur.

The alternate appliance is ready for use.

Managing the Alternate Appliance

Some management operations are disabled for an alternate appliance.

The management operations that can be performed on an alternate appliance include:

- Login.
- Uploading software.
- Downloading all types of log files.
- Restarting and shutting down the service or the appliance.
- Setting as a primary appliance.
- Uploading an SSL certificate for Web Services operation in the alternate appliance. This operation uploads the SSL certificate also for a RESTful based Web Services interface.
- Monitoring the performance of the appliance.

Note: You can also optionally set an alternate appliance as the primary appliance. For more information refer to [Setting an Alternate Appliance to be the Primary Appliance](#).

These management operations are available from the ARX CoSign Appliance Management window of the Administration MMC (refer to [Chapter 5: Managing the DocuSign Signature Appliance](#)).

Note: An alternate appliance cannot be backed up. If the appliance fails, it should be re-installed as specified in [Installing an Alternate DocuSign Signature Appliance](#).

Note: If the primary appliance fails and is later re-installed from backup, all alternate appliances must be re-installed as well.

Managing Data Replication in the Alternate Appliance

You can view and manage data replication using the Administration MMC. The information can be expanded from the primary appliance information. It is important to view the replication status after the conclusion of alternate appliance installation, since the replication procedure continues after installation is complete.

To view and manage data replication, select **Subscribed Alternates** under the primary appliance. The *Subscribed Alternates* window that appears lists the alternate appliances.

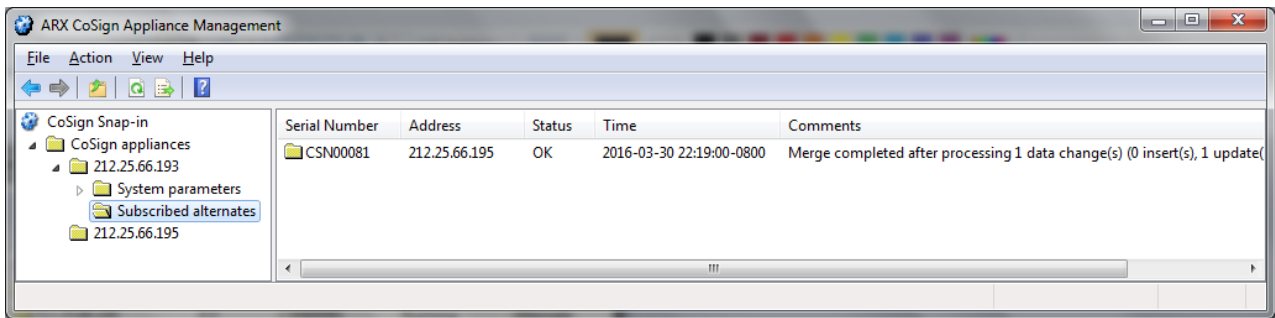


Figure 86 Subscribed Alternates Window

For every alternate appliance in the Subscribed Alternates window, you can:

- View replication status, in addition to other information about the alternate appliance.
- Re-initialize the alternate appliance, i.e., force a replication operation.
- Unsubscribe an alternate appliance. This removes the alternate appliance from the list of subscribed alternates.

Viewing Replication Status of an Alternate Appliance

The Subscribed Alternates window (Figure 86) in the Administration MMC displays the time of the last replication activity accompanied by descriptive text. It also displays the following information about each alternate appliance: the Serial Number, the IP Address and the Status.

The possible statuses include:

- **OK** – No data needs updating in the alternate appliance.
- **Running** – The alternate appliance is currently synchronizing with the database of the primary appliance.
- **Retrying** – The primary appliance is trying to communicate with the alternate appliance, but cannot reach it due to network problems or because the alternate appliance is not installed.
- **Failed** – Replication has failed. This occurs after several failed retry attempts.

Re-initializing an Alternate Appliance

The Subscribed Alternates window in the Administration MMC enables re-initializing an alternate appliance. This forces a replication operation in which all the relevant data of the primary appliance is copied to the alternate appliance.

Re-initialization can be used in cases where replication failed due to transient network problems.

To re-initialize an alternate appliance:

- In the **Subscribed Alternates** window (Figure 86), right-click the appliance you wish to re-initialize.
- From the popup menu, select **All Tasks** → **Re-initialize**.

Unsubscribing an Alternate Appliance

The Subscribed Alternates window in the Administration MMC enables unsubscribing an alternate appliance. This removes the **alternate** appliance from the list of Subscribed Alternates. Use this option when an alternate appliance is no longer relevant in the site of the primary appliance, or before re-installing the alternate appliance.

To unsubscribe an alternate appliance:

- In the **Subscribed Alternates** window (Figure 86), right-click the appliance you wish to unsubscribe.
- From the popup menu, select **All Tasks** → **Unsubscribe**.
- At the prompt, confirm the operation.

Managing Primary Appliance Failure and Recovery

In cases of severe hardware failure in a primary appliance, you can set one of the alternate appliances to be the primary appliance. The selected appliance is now the primary appliance of the cluster. It can replicate its data to all the alternate appliances in the high availability cluster. The previous primary appliance is no longer a member of the high availability cluster. When the failed primary appliance recovers, you can re-define it as an alternate appliance in the cluster.

Setting an Alternate Appliance to be the Primary Appliance

In the case of severe hardware failure in a primary appliance, you should define an existing alternate appliance as the primary appliance.

There are several reasons why it is advisable to have an up and running primary appliance available in a high availability cluster. These include:

- In a Directory Independent environment, you can add or update users only via the primary appliance.
- In an Active Directory or LDAP environment, you can synchronize with the domain only via the primary appliance.
- You can interface with the automated external CA only via the primary appliance.
- You can perform administrative operations only via the primary appliance. When the primary appliance is down, no administrative activity such as downloading a backup file is possible.

Before setting the alternate appliance as a primary appliance, you must ensure that all configuration settings that were defined in the environment of the primary appliance are also defined in the environment of the alternate appliance. For example, if the system is configured to use an automatic external CA, the primary appliance was given network access to the external CA. You should make sure that the alternate appliance is also able to access the automatic external CA.

To set an alternate appliance to be the primary appliance:

Caution: Make sure that there are no network disconnections or power failures during the following procedure.

- In the *ARX CoSign Appliance Management* window (Figure 85), right-click the alternate appliance you wish to set as primary.
- From the popup menu, select **All Tasks** → **High Availability** → **Set as Primary**.

The *Set as Primary* window appears. The **Cluster status** section displays the current configuration of the cluster.

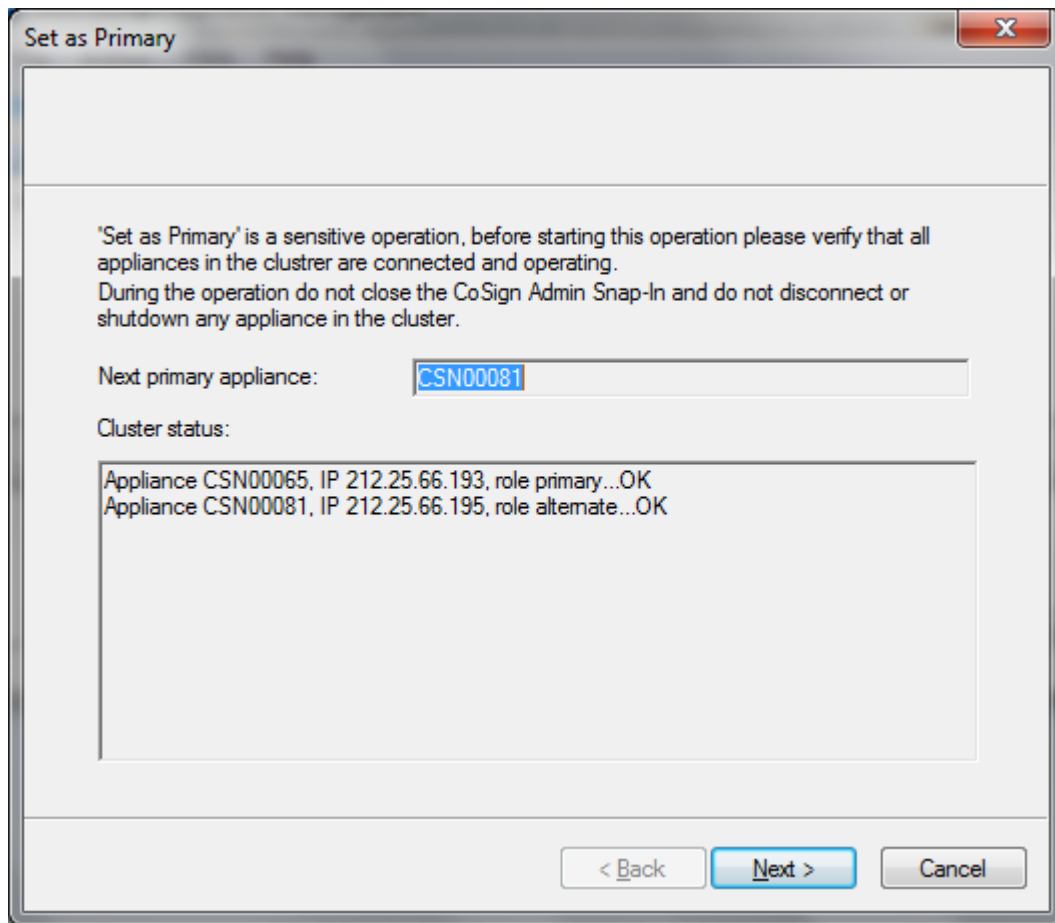


Figure 87 Set as Primary – Cluster Status

- Click **Next** and confirm the operation.

A progress window appears, and the operation of switching the role of primary to the alternate appliance begins.

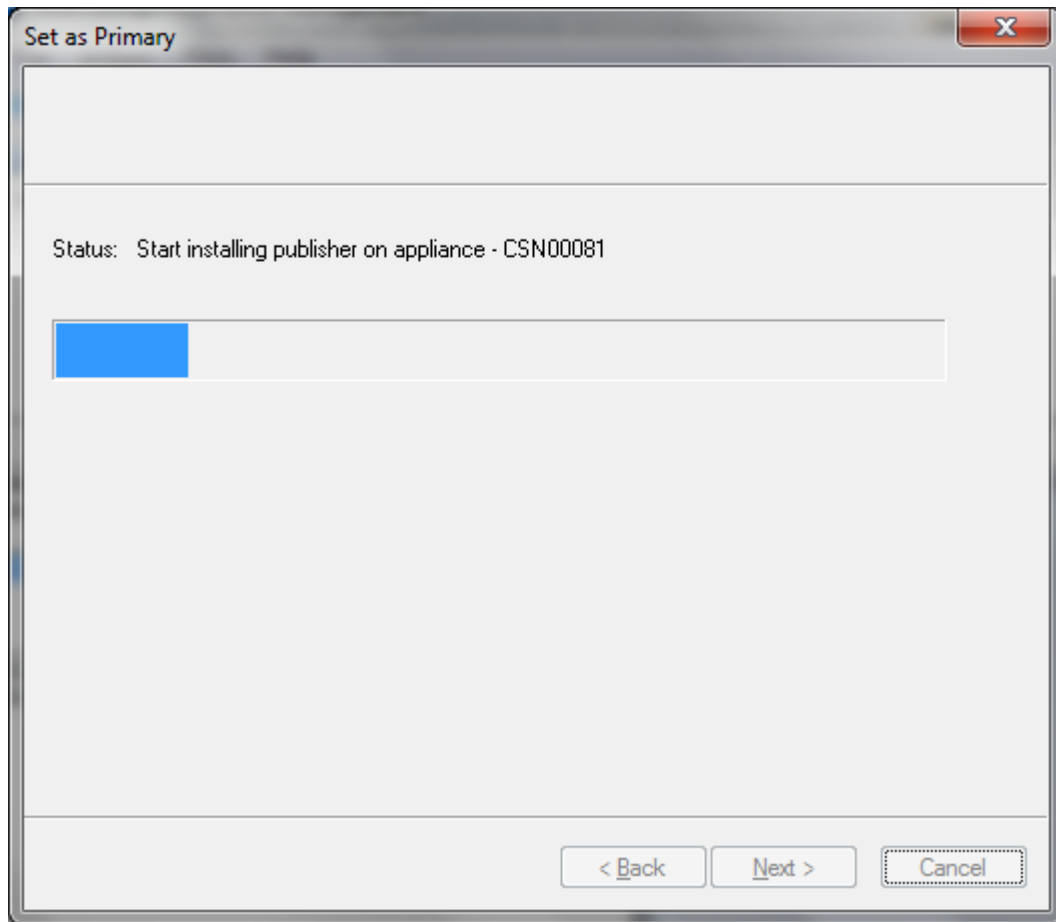


Figure 88 Set as Primary – Start installing the alternate as a primary

At the end of the operation a report is displayed, describing the performed actions. If you suspect any failure in the operation, contact ARX support at <http://www.arx.com/support/supportrequest>.

- Click **Finish**.

The selected appliance is now the primary appliance of the cluster. It can replicate its data to all the alternate appliances in the high availability cluster.

Note: There can only be one primary appliance in a cluster. If the previous primary appliance becomes operational again, you can define it as an alternate appliance (refer to [Setting a Previous Primary Appliance to be an Alternate Appliance](#)).

Setting a Previous Primary Appliance to be an Alternate Appliance

You can set a previous primary appliance to be an alternate appliance. This is useful for cases where a previously-defined primary appliance that failed becomes operational again, and you wish to add it the cluster as an alternate appliance.

To set a previous primary appliance to be an alternate appliance:

- In the *ARX CoSign Appliance Management* window (Figure 85), right-click the previous primary appliance that you wish to designate as an alternate.
- From the popup menu, select **All Tasks** → **High Availability** → **Subscribe as Alternate**.

After you confirm the operation, the previous primary appliance will become an alternate appliance.

Resubscribing an Alternate Appliance with a Primary Appliance

There are cases where an alternate appliance is unsubscribed from a primary appliance, and you wish to resubscribe it with the primary appliance. For example, the alternate appliance is being upgraded. Note that you can resubscribe an alternate appliance to the primary appliance, without having to re-install the alternate appliance.

To subscribe an alternate appliance with a primary appliance:

- In the *ARX CoSign Appliance Management* window (Figure 85), right-click the primary appliance to which you wish to subscribe an alternate appliance.
- From the popup menu, select **All Tasks** → **High Availability** → **Subscribe Alternate to Primary**. You are prompted to supply the IP address of the alternate appliance.
- Enter the IP address of the alternate appliance.
- Confirm the operation.

After several seconds the operation is completed and the specified appliance is added to the alternates list of the primary appliance.

Upgrading Appliances Participating in a High Availability Cluster

Note: All appliances participating in a high availability cluster must run the same version of DocuSign Signature Appliance.

To upgrade appliances in a high availability cluster:

- Unsubscribe all alternate appliances from the primary appliance (refer to [Unsubscribing an Alternate Appliance](#)).
- In the Subscribed Alternates window ([Figure 86](#)), make sure that no alternate appliances are listed for the primary appliance.
- Upgrade the primary appliance (refer to [Upgrading](#)). Wait until the upgrade is complete.
- Upgrade all the alternate appliances to the same version as the primary appliance.

In each alternate appliance, verify that the upgrade has completed successfully and that the console shows the updated version number.

- Subscribe each alternate appliance to the primary appliance (refer to [Resubscribing an Alternate Appliance with a Primary Appliance](#)).

The high availability cluster is now upgraded and ready for operation.

Chapter 8: Configuration Utility

The client behavior in general and each component in particular have several modes of operation that are suitable for different kinds of usage and customer needs. These different modes of operation can be set by the user, or can be set and then distributed by the organization's administrator.

The Configuration Utility enables both the user and the administrator to set the configuration of any parameter in any of the client components both for a single machine and for a group of machines.

User related functionality is described in the *DocuSign Signature Appliance Client User Guide*.

Overview

The Configuration Utility is a GUI application that enables a user or administrator to set any of the client components' configurable parameters easily and intuitively.

The Configuration Utility can run in either of two modes:

- *Admin* mode is run by an administrator to build a certain setting for distribution. It can be a registry file or a group policy that can be distributed to different clients by the Active Directory group policy mechanism, using login scripts or manually.
- *End User* mode allows a user (or administrator) to view or configure the client behavior on the machine on which the utility is running.

The utility displays a components tree, in which you can select the component whose configuration values you wish to set. Each component includes several independent groups of parameters, which can be independently set.

The utility can also be used on a specific machine to view or update the current configuration. This may be useful for debugging purposes or when the client behavior deviates from the expected.

Note: The Configuration utility is not the only method for changing the client's behavior. Some of the components have their own GUI for setting their own configuration (such as the ARX Legacy Word Add-in plug-in, OmniSign, and others), but while the components' GUI changes the setting of the current user, the Configuration utility changes the configuration of the local machine.

You can also use the Configuration Utility to retrieve the internal CA certificate and the CA CRL (Certificate Revocation List).

Using the Configuration Utility

The Configuration Utility enables you to view and edit all the configurable parameters of the client components. In *End User* mode, only the installed components are displayed, while in *Admin* mode you can view and change the settings of all the client components. Refer to [Running the Configuration Utility in Admin Mode](#) and [Running the Configuration Utility in End User Mode](#) for more information about the two modes.

To run the Configuration Utility:

- To run in **Admin** mode, select **Start > Programs > ARX CoSign > CoSign control panel**. The CoSign Control Panel appears (Figure 34). Select the Client Configuration Management item. The configuration utility main window appears.

- To run in **End User** mode, select **Start > Programs > ARX CoSign > CoSign Control Panel**. The Control panel appears (Figure 34). Select the Client Configuration item. The configuration utility main window appears.

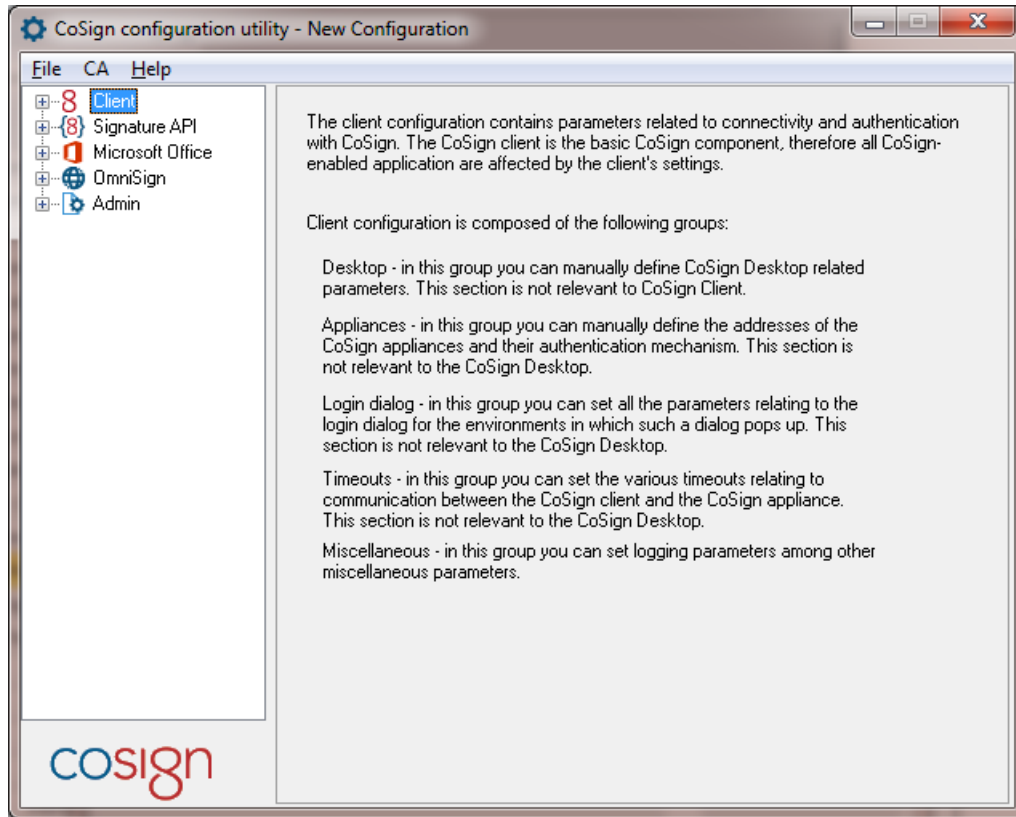



Figure 89 CoSign Configuration Utility – Main Window

The left pane of the Configuration Utility displays a components tree. Each node in the highest level of the tree is a configurable client component. Each component has one or more sub-nodes, with each sub-node being a group of parameters. These sub-nodes group parameters by category, except for the Miscellaneous sub-node, which includes all the parameters that are not included in any of the other groups.

To edit a parameter:

- Double-click the component to which this parameter belongs, or click  to the left of the component. The component's sub-nodes are displayed.
- Select the sub-node that contains the parameter. The right pane displays all the configurable parameters for the sub-node.

The right pane of each sub-node (except **Miscellaneous**) displays all the configurable parameters, with a triplet of radio buttons on top. Since the **Miscellaneous** group is a collection of various unrelated parameters, it may display several triplets, one for each logical set of parameters.

- Select one of the radio button options:
 - **Not Configured** – When this option is selected, the local machine definition of this sub-node's parameters remains unchanged when the configuration is applied to the local machine. When this option is selected, the parameters are greyed out and you cannot edit them.

- **Use Defaults** – When this option is selected, registry entries for all this sub-node’s parameters are removed when the configuration is applied to the local machine, and the defaults are used. When this option is selected, the parameters are greyed out and you cannot edit them.
- **Set <Sub-node Name> Parameters** – When this option is selected, the sub-node’s parameters become editable and display values where applicable (either the default value or a value taken from the local machine definition). When the configuration is applied to the local machine, **all** the parameters of this group are written to the registry. New registry keys and values will be created if necessary, and the old values, if defined, are overwritten.

You can configure parameters for the following components:

- ◆ *Client*. For explanations about the configurable parameters, refer to the Configuration Utility chapter in the *DocuSign Signature Appliance User Guide*.
- ◆ *Signature API*. For explanations about the configurable parameters, refer to the Configuration Utility chapter in the *DocuSign Signature Appliance User Guide*.
- ◆ *Microsoft Office*. For explanations about the configurable parameters, refer to the Configuration Utility chapter in the *DocuSign Signature Appliance User Guide*.
- ◆ *OmniSign*. For explanations about the configurable parameters, refer to the Configuration Utility chapter in the *DocuSign Signature Appliance User Guide*.
- ◆ *Admin*. For explanations about the configurable parameters, refer to [Setting Admin Configuration](#).

Configuration Utility Menus

The following sections describe the menu options available from the Configuration Utility: **File**, **CA**, and **Help**. Note that the **File** menu differs for Admin mode and End User mode.

File Menu – Admin Mode

The following options are available in Admin mode from the **File** drop-down menu:

Note: For a detailed explanation of configuration file operations and group policy operations, refer to [Configuration File Operations](#) and [Group Policies Operations](#).

New Configuration

Enables creating a new configuration file.

Open

Enables opening and importing a configuration file. All the settings defined in the file are displayed in the relevant components’ dialogs. The components and values that are not defined in the file appear with the **Not configured** option selected.

You can import either from a file or from a Group Policy.

Save

Enables saving a configuration file.

Save configuration file as

Enables saving a configuration file as a new configuration file.

Export to configuration file

Enables exporting to a configuration file only when working on Group Policy settings. You must specify the desired file name and location.

Exporting allows the administrator to distribute a specific configuration manually, or via login scripts or other distribution mechanisms that allow working with `.reg` files.

You can generate a file that is suitable either for a 32 bit Windows System or for a 64 bit Windows System.

Export to group policy

Enables exporting the configuration file to an existing Group Policy. Select the Group Policy to which the settings should apply.

You can generate a file that is suitable either for a 32 bit Windows System or for a 64 bit Windows System.

CA Menu

The following options are available from the **CA** drop-down menu:

Install CA Certificate

Enables installing the ROOT certificate into the current user's PC. Refer to [Chapter 4: Deploying the DocuSign Signature Appliance Client](#) for information relating to the ROOT certificate.

Download CA Certificate

This option is very similar to the **Install CoSign CA Certificate** option. The difference is that in this case the ROOT CA certificate is output to a selected file. The downloaded file can be placed in the AIA location according to the AIA field defined in the users' certificates.

Download CA CRL

Enables downloading the CRL (Certificate Revocation List) to a file. The downloaded file can be placed in the CDP (CRL Distribution Point) location according to the CDP field defined in the users' certificates.

Help Menu

The following options are available from the **Help** drop-down menu:

About

Displays the version of the configuration utility as well as a link to the ARX web site.

Contents

Displays the content of this chapter in on-line help format.

Create report

Enables generating a report listing information on both the Client installation and the appliance installation. Click **Save** to save the report to a file. The file can be sent to ARX support for problem analysis.

The report includes three parts:

- Client installation files – Includes all the files of the installation, their dates, sizes and version information.

- Client and Server parameters – Includes Client and Server parameters. The parameters also include information that is displayed in the console.
- Environmental information – Displays information about the PC in which the client is installed, the version of the installed MS Office application, and other parameters that can be valuable to ARX support for problem analysis.

Running the Configuration Utility in Admin Mode

Note: To run the Configuration Utility in Admin mode, you must first install the admin client. Refer to [Installing DocuSign Signature Appliance in a Directory Independent Environment](#).

To run the Configuration Utility in Admin mode:

- Select **Start > Programs > ARX CoSign > CoSign control panel**. The Control Panel appears. Select the Client Configuration Management item.

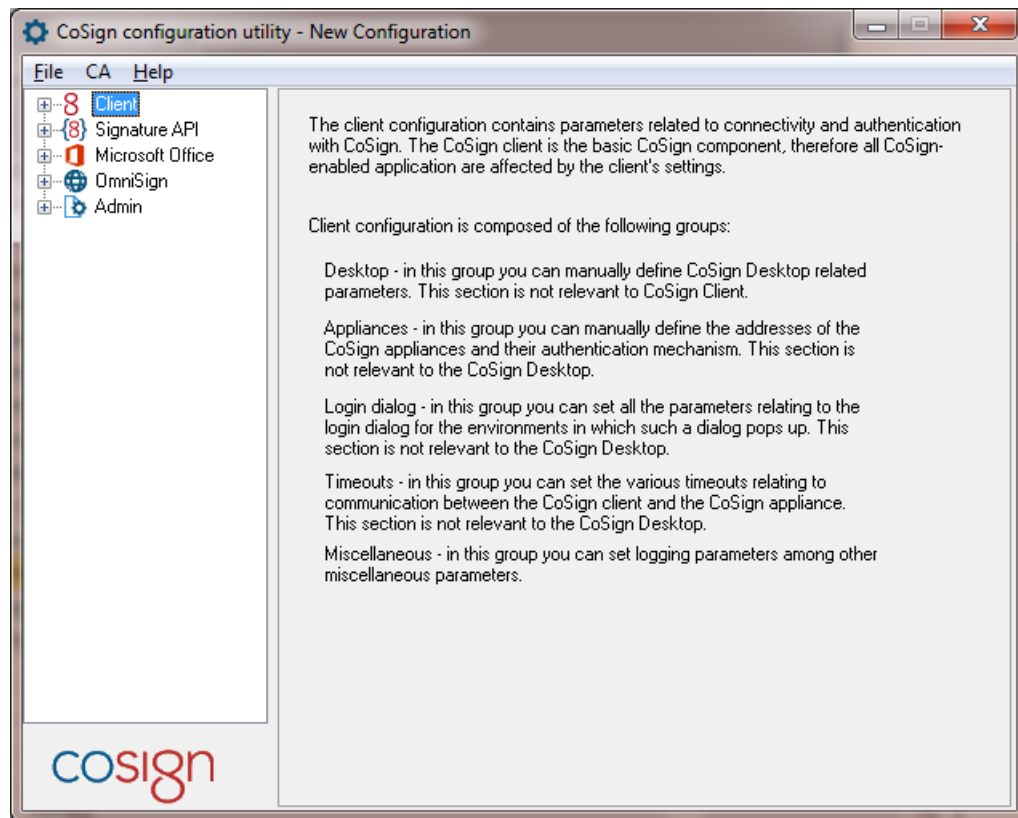


Figure 90 Client Configuration Utility – Admin Mode

- Edit the parameters as described in [Using the Configuration Utility](#).

When running in *Admin* mode, all the client configurable components are displayed in the left pane, regardless of the components installed on the machine you are working on.

The application starts with a new configuration file whose components are all non-configured. You can either edit this new configuration or you can open an existing configuration from a file or from Group Policy.

The *Admin* mode of the Configuration Utility enables administrators to create and edit configuration files and to add and edit client configuration to an existing Active Directory Group Policy.

The configuration files are actually valid registry files that can either be imported to an end user machine (by double-clicking them or from **regedit**), or can later be used as input to the configuration utility (in *Admin* mode) for further editing or for exporting to Group Policy, or can be imported by the Configuration Utility (in *End User* mode) for configuring a single machine's settings.

You can perform the following when running the Configuration Utility in *Admin* mode:

- ◆ Edit and save a configuration file.
- ◆ Edit/view a configuration file and export the client settings to an existing Active Directory Group Policy.
- ◆ Edit/view the settings of a Group Policy and save them in the same Group Policy or export them to another Group Policy.
- ◆ Edit/view the settings of a Group Policy and export them to a configuration file.
- ◆ Install/Download the CA certificate. Refer to [Install CA Certificate](#) and [Download CA Certificate](#).
- ◆ Download the CA CRL (Certificate Revocation List). Refer to [Download CA CRL](#).

The following sections describe basic Configuration File and Group Policy operations.

Configuration File Operations

The following sections describe basic configuration file operations.

Creating a New Configuration File

A new configuration file can be created in either of two ways:

- When the application starts it always starts with a new configuration file.
- By selecting **File > New configuration**.

After changing all desired parameters, you must either:

- Save the configuration file – select either **File > Save** or **File > Save configuration file as**.
- Export the configuration file to an existing Group Policy (refer to [Exporting to a Group Policy](#)).

Opening a Configuration File

A configuration file is typically opened for one of two reasons:

- For editing and saving.
- For viewing and exporting to an existing Group Policy.

To open a configuration file, select **File > Open**. All the settings defined in the file are displayed in the relevant components' dialogs. The components and values that are not defined in the file appear with the **Not configured** option selected.

Exporting to a Configuration File

When in *Admin* mode, you can export to a configuration file only when working on Group Policy settings. Exporting allows the administrator to distribute a specific configuration manually, or via login scripts or other distribution mechanisms that allow working with `.reg` files.

To export a Group Policy setting to a configuration file, select **File > Export to configuration file**, and browse for the desired file name and location.

Group Policies Operations

When opening and exporting group policies, a list of the available policies is displayed according to the current user's credentials and the domain to which the current machine is joined. This list contains all the domain's group policies which the user may view/edit, as well as all the group policies defined for the local machine which the user may view/edit.

The Configuration Utility enables you to view and edit related parameters in a Group Policy.

Opening a Group Policy

The Configuration Utility can be used to open and edit the setting in an existing Group Policy. Note that only the specific settings are retrieved from the Group Policy and thus only these settings can be edited or viewed.

To open a Group Policy for editing, select **File > Open group policy**. A list of all the available group policies is displayed. Select a group policy, and all its defined settings are displayed in the relevant components' dialogs. The components and values that are not defined in the policy appear with the **Not configured** option selected. Specifically, if you open a Group Policy that never contained definitions, all values of all components appear with the **Not configured** option selected.

After setting (or viewing) the desired values, you can either save the settings to the Group Policy, or export the values to a configuration file or to another Group Policy. Refer to [Exporting to a Group Policy](#) and [Exporting to a Configuration File](#), respectively, for how to export the configuration values.

Exporting to a Group Policy

Exporting to a Group Policy is typically performed in either of two situations:

- When you work on a Group Policy's settings and wish to apply the settings to another Policy.
- When you work on a configuration file and wish to apply the settings to a Group Policy.

To export configuration settings to a Group Policy, select **File > Export to group policy**, and select the Group Policy to which the settings should apply.

Note: After exporting the settings to a Group Policy, additional changes are saved to the original file or policy and not to the one to which the settings were exported.

Running the Configuration Utility in End User Mode

The Configuration Utility can also be used for editing and viewing a specific machine's settings. When the application runs in *End User* mode, it looks for all the components that are installed, and for each component reads its settings and displays them in the relevant dialog. For more information, refer to the *DocuSign Signature Appliance User Guide*.

Distributing the Client Configuration

The client consists of several components, which can be operated in different modes according to organizational needs. These modes can be controlled by the component's parameters.

While in some organizations there is a policy of how things should work and look like, and therefore all users must have the same configuration, there are some other organizations where there is more than one such policy for the different organizational units, and others where there is no policy at all and every user can determine his/her own configuration.

All components are installed with a default behavior that should fit most users. Some components have their own GUI for changing the default configuration, and the client configuration can also be centrally set using a configuration file or Group Policy. Following is a list of the common ways to set and distribute client configurations:

- Use defaults – Do nothing except install the client from the CoSign CD. All users will have the same default behavior.
- Use the components' GUI – For each configured machine, use the components' GUI to configure each component (Office Signature plug-in, OmniSign) as desired. Refer to the chapters describing the component's GUI for an explanation of the various parameters and how to configure them.
- Use the Configuration Utility in *End User* mode – Run the Configuration Utility on each machine you wish to configure and set the parameters as desired.
- Use Configuration files – Use configuration files that are created by the Configuration Utility. Refer to [Distributing the Configuration Using Configuration Files](#) below.
- Use Group Policy – In an Active Directory environment you can use Group Policies for distributing different configurations to different groups of machines. Refer to [Distributing the Configuration Using Group Policy](#).

Distributing the Configuration Using Configuration Files

The configuration files created by the Configuration Utility are actually valid `.reg` files. You can create these files in *Admin* mode (refer to [Creating a New Configuration File](#)), or by exporting a certain machine's setting.

Once the configuration file is created you can distribute it in any of the following ways:

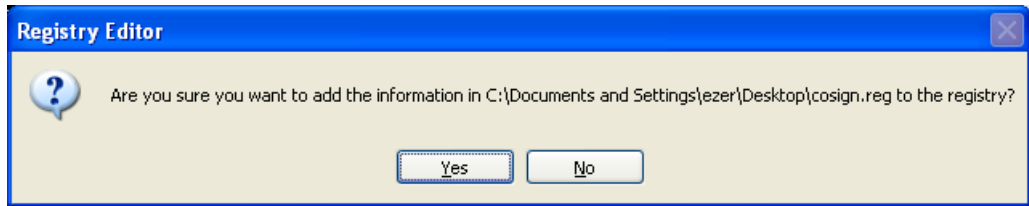
- Manually – Refer to [Distributing the Configuration Manually](#).
- Using Login Scripts or other distributing software – Refer to [Distributing the Configuration via Login Scripts or any Distributing Software](#).

Distributing the Configuration Manually

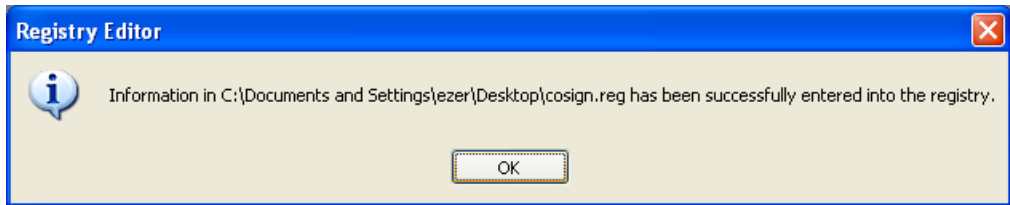
Note: You must have administrative rights on the machine in order to apply the configuration values.

To distribute the configuration manually:

- Copy the appropriate `.reg` file to the machine for which you want these settings to apply.
- Double-click the file. A message pops up, requesting confirmation to apply the new registry values.



- Click **Yes**, and wait for the message confirming that the operation was completed successfully.



- Click **OK**.

Note: Some components must be restarted in order for the new configuration to take effect, or else they will keep working with the old settings. It is recommended to restart the machine after manually installing a new configuration.

Distributing the Configuration via Login Scripts or any Distributing Software

Since the configuration file is a `.reg` file that changes some settings in HKLM, any software or tool that is able to apply `.reg` files and has the appropriate access rights on the target machine can be used to distribute the configuration files.

Distributing the Configuration Using Group Policy

In an Active Directory environment, you can distribute the configuration using a Group Policy. You can use one Group Policy for all your users, or you can have several policies for several organizational units.

configuration values do not require a proprietary Group Policy, but are integrated in existing policies.

When opening a Group Policy in the Configuration Utility, the application retrieves only the related parameters and displays them in the relevant dialogs. When saving the configuration, or when exporting it to a specific Group Policy, the application removes all the related definitions from the existing policy, and replaces them with the new settings. All non-related definitions are not affected by the saving/exporting action.

Both the opening and the saving operations show the user all existing Group Policies available to the user according to the user's credentials; you cannot use the Configuration Utility to create a new policy.

Setting Admin Configuration

Admin configuration enables you to set parameters relating to the appliance installation. Some of these parameters affect the appliance itself, while others configure the administrator's machine installation capabilities.

Admin – Appliance Installation

This group enables you to set parameters that relate to the appliance installation. You can set the log level and the administrators group defined within the appliance, as well as the administrator's machine

installation capabilities, such as in which types of directories you can install DocuSign Signature Appliance, and whether you may set AIA and CDP in the internal CA setup.

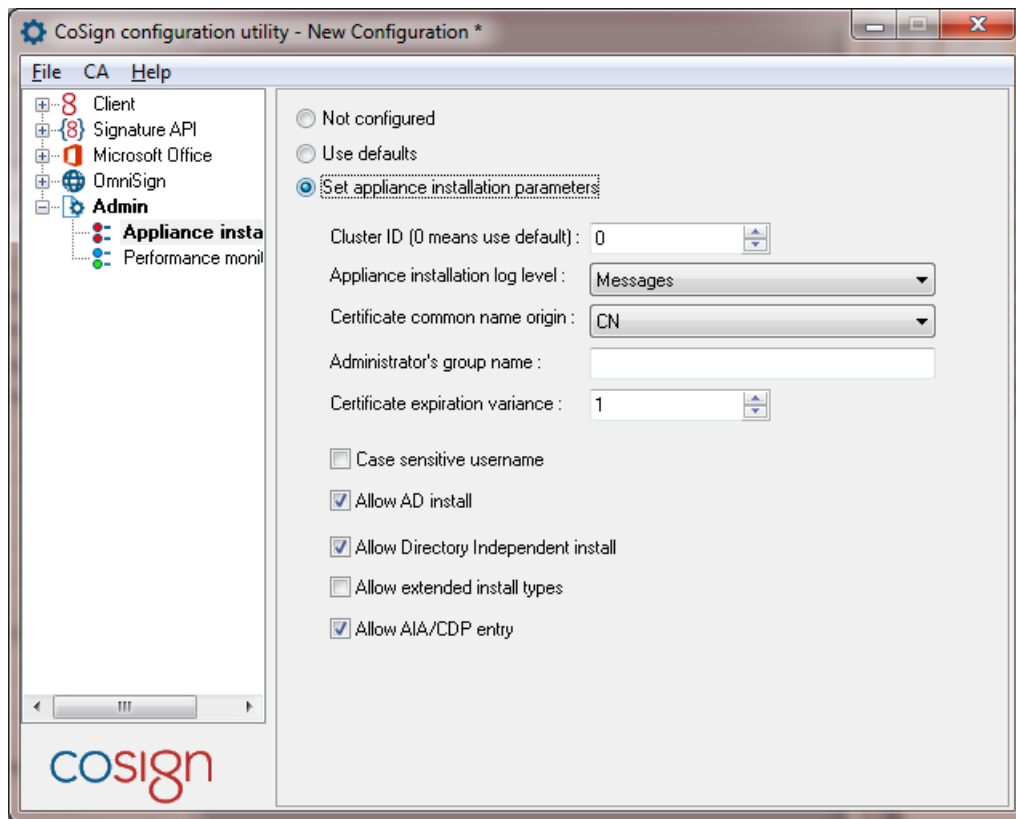


Figure 91 Configuring Admin – Appliance Installation Parameters

In the **Appliance Installation** group you can set the following Admin parameters:

Appliance related settings:

- *Cluster ID (0 means use default)* – Do not change this value unless instructed to do so by ARX technical support.
- *Appliance installation log level* – Specify the reporting level of the appliance to the log while installation is in progress. It is recommended not to change this setting.

Certificate common name origin – Directs how to define the Common Name field in the created user certificate. The origin can be either the common name of the user in the directory or the display name of the user in the directory.

This parameter is identical to the *Certificate Common Name* parameter in the system parameters.

- *Administrator's group name* – Specify the name of the directory service's user group that identifies authorized administrators. You can select any name for this group. Make sure that all users who perform administrative tasks are assigned to this group.
Default value: administrators.
- *Certificate expiration variance* – The maximum number of days that may be subtracted from the certificate's expiration date for the purpose of refreshing the certificate.
This parameter is identical to the *Certificate Expiration Variance* parameter in the system parameters

- *Username case sensitive* – Check this option if you wish the login username to be case sensitive. The new setting takes effect after the upcoming installation. The default value is case insensitive. This parameter is relevant for a installation in a Directory Independent environment.

Administrator's machine related settings:

- *Allow AD install* – Check this option to enable the administrator to install appliance in an Active Directory environment.
- *Allow Directory Independent install* – Check this option to enable the administrator to install appliance in a Directory independent environment.
- *Allow extended install types* – This option should always remain unchecked.
- *Allow AIA/CDP entry* – Check this option to enable the administrator to change the AIA and CDP fields in the CA setup dialog.

Admin – Performance Monitoring

Change the settings only if instructed to do so by ARX.

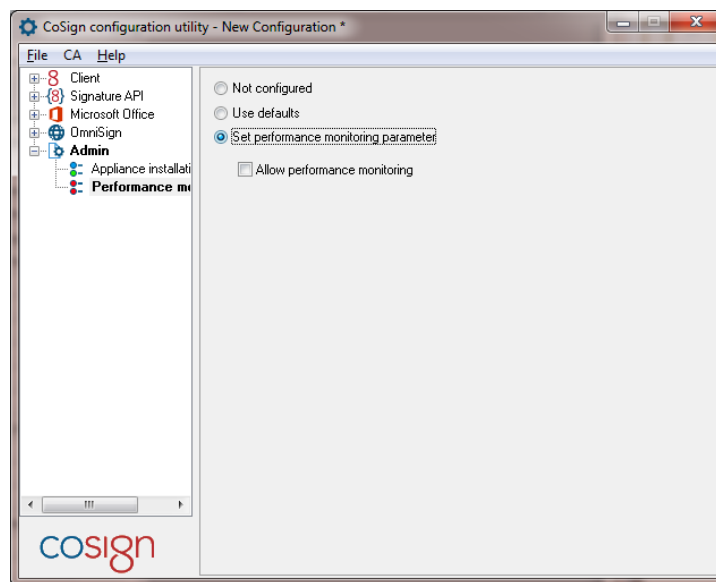


Figure 92 Configuring Admin – Performance Monitoring Parameters

Chapter 9: Troubleshooting

This chapter offers solutions to various problems you may encounter while installing or running the appliance.

If you are unable to identify or solve a problem, try the DocuSign Support Center at <https://support.docusign.com> and look for the DocuSign Signature Appliance.

DocuSign Support information

DocuSign Support Center <https://support.docusign.com>

Support Contact page <https://support.docusign.com/contactSupport>

Installation Problems

This section describes various problems and error messages you may encounter during the installation process, and provides possible solutions to these problems.

IP Address is Invalid

Problem: During software installation, this message appears after you enter the address and click **Next**.

Solution: This message indicates that DocuSign Signature Appliance is not accessible. Perform the following:

- Verify that the IP address you entered is correct.
- Verify that DocuSign Signature Appliance is operational.
- Check for networking problems.

Error When Setting the IP Address Via the Console Interface

Problem: When setting the IP address through the console, one of the following error messages appear: **failed error 51**, **failed error 52**, or **failed error 54**.

Solution: Check the following:

- Verify that DocuSign Signature Appliance is properly connected to the network. Verify there are no switch problems, cable problems, etc.
- Verify that the IP address you entered is not being used by another machine in the network. One way to check this is to ping the IP address; if you receive an answer, it means that the IP address is being used by another machine in the network.
- If the problem is none of the above and the network has a DHCP server installed, perform the following:
 - Choose the **Use DHCP** option in the console main screen.
 - Restart the appliance.

- Select **Ip Addr** in the console main screen to view the IP address that was allocated by the DHCP server.
- Perform **Save**. The Appliance saves as static IP the address that was allocated by the DHCP server.
- Remove this IP address from the IP addresses pool of the DHCP server.

Default Values Do Not Appear in the Directory Setup Dialog Box

Problem: During software installation, the *Directory Setup* dialog box appears without any default values.

Solution: DNS configuration may be problematic, causing an installation failure. For more information, refer to [Installation Failed](#).

The Appliance is Not in Factory Settings Mode

Problem: During software installation, this message appears after you enter the address and click **Next**.

Solution: This message indicates that a DocuSign Signature Appliance with the IP address entered is already installed. Perform one of the following options:

- Enter a different IP address.
- Return DocuSign Signature Appliance to factory settings using the console, and then rerun the installation process.

Note: Since this message indicates that DocuSign Signature Appliance is already installed, you may want to cancel the installation process to prevent the accidental reinstallation of DocuSign Signature Appliance.

Installation Failed

Problem: The software installation process fails.

Solution: Verify the following:

- DNS supports dynamic updates. This information is included in the DNS server properties.
- The user running the Administration MMC has the necessary privileges. The user must be a member of both the `domain admins` and `enterprise admins` groups.

If you have verified all of the above, and the installation process still fails, download the Install log. For information on downloading the Install log, refer to [Downloading Log Files](#).

The Install log may include one of the following errors:

- Failed to join the domain – If this error appears in the Install log, verify the following:
 - ◆ The domain controller is up.
 - ◆ The domain name was entered correctly.
 - ◆ The administrator user has the necessary privileges to register computers to the domain.
- Failed to remove http URLs for CDP and AIA – This error usually indicates a failure in CA installation. Send the Install log file to ARX technical support (support@arx.com).

Progress Bar Stops Advancing

Problem: During software installation, the progress bar stops advancing at the user's keys and certificate generation stage, and only one user is defined in DocuSign Signature Appliance.

Solution: There may be a DNS configuration problem (in either DHCP or static IP mode). Perform the following:

- Do **not** close the installation wizard.
- Modify the DNS Server IP address from the console. The progress bar will continue advancing until the installation is completed.

Appliance Installation Issues

Problem: In an MS Active Directory environment, right after the installation starts, the following error appears: "Installation failed in step 93 with reason: failed to join the domain, error code is 1231". Sometimes the error code is 1355.

Cause: The appliance failed to join the domain due to network configuration problems.

Solution: Check for network setting such as DNS IP on the console. Make sure to restart the appliance after any changes to the IP or DNS even if the change was successful.

To be sure that your network configuration is OK try to ping with the appliance IP using the `-a` option. You should get a reply with the appliance full DNS name.

High Availability/Load Balancing – Alternate Installation

Problem: After completing the installation of an alternate appliance, the following message appears in the subscribed alternate: "The snapshot for this publication has become obsolete".

Cause: You did not restart the primary appliance before starting the alternate installation.

Solution:

- Unsubscribe the alternate appliance.
- Restore the alternate to factory settings.
- Restart the primary appliance (hardware restart).
- Re-install the alternate appliance.

Appliance Problems

Appliance Does Not Start

Problem 1: Even though power is on, the appliance shows no sign of being on. The power LED is off.

- **Solution 1:** Check that the power cables are indeed connected to the power supply.

Problem 2: The power LED is on. The Console does not stop displaying the message: *CoSign is now starting, please wait*. Even after restarting several times the same message continues to display.

- **Solution 2:** Follow the instructions in [Restoring the Appliance After an Internal Hard Disk Failure](#). It is recommended to consult with ARX technical support before carrying out the instructions.

Console Problems

The console provides messages and alerts for the following problems (refer to [System Does Not Respond](#) for more information):

- [Tamper] – A tamper event occurred.
- [License] – There is a problem with the license MiniKey.
- [IP Addr] – The appliance does not have an IP address.

Following are licensing issue messages that can also appear in the console:

- Passed 90% of license limit – Contact ARX to obtain a larger license.
- Appliance license is not present, please insert your license MiniKey. Warning <num> of 5, system will shutdown! – The license MiniKey is not inserted. Insert the MiniKey immediately.
- The amount of users in the appliance has passed the license limit. Warning <num> of 5, system will shutdown! – Either obtain a new license MiniKey or remove users from the scope of users.
- An improper license Minikey is inserted(<error-code>). Warning <num> of 5, system will shutdown! – Insert a proper license MiniKey.

For more information on licensing issues, refer to [New Users Do Not Receive Certificates](#).

Client-Related Problems

This section describes various problems and error messages you may encounter while running the Client, and provides possible solutions to these problems.

Cannot Enable the “Add Digital Signature to Outgoing Messages” Checkbox in Outlook

Problem: In Microsoft Outlook, the **Add digital signature to outgoing messages** checkbox is disabled.

Solution: In order to send signed emails, you must first define security settings. Refer to *Signing Outlook Emails* in the *DocuSign Signature Appliance User Guide*.

Cannot See Any Certificates in Store

Problem: You cannot see any certificates in your Microsoft Personal certificates store.

Solution: Perform the following:

- Restart the machine and try again.
- Verify the following:
 - You are logged in to the same domain. You should not be logged in to any other domain, and you should not be logged in to the current machine.

- Your DNS definitions are correctly configured on the PC. These definitions should be the same as the domain's DNS.
- You receive a response when you ping the IP address or try to connect to DocuSign Signature Appliance using telnet to port 443.
- Your user account is defined in the directory that was defined as the AD users container during installation (refer to [Figure 12](#)).
- If you are using a Directory Independent environment, you did not omit to set configuration parameters for the client machine. Use the **Configuration Utility** to setup the appliance IP address (refer to the Client – Appliances section in the Configuration Utility chapter of the *DocuSign Signature Appliance Administrator Guide*).

Administrative Problems

This section describes various problems and error messages you may encounter while managing DocuSign Signature Appliance, and provides possible solutions to these problems.

System Parameters Do Not Appear in the Administration MMC

Problem: You do not see any system parameters in the Administration MMC.

Solution: In order to perform administrative operations using the Administration MMC, you must be a member of the Administrators group. This group is defined in the **Administrator Group** system parameter, and its default value is `Administrators`. The **Administrator Group** parameter is displayed in the Console (refer to [Chapter 6: Using the Consoles](#)).

All Administration MMC Operations Fail

Problem: Any operation you attempt to perform in the Administration MMC fails.

Solution: Refer to [System Parameters Do Not Appear in the Administration MMC](#).

System Does Not Respond

Problem: You cannot access DocuSign Signature Appliance through the Administration MMC or perform digital signature operations.

Solution: Check the appliance status. The cause may be one of the following:

- A correct license MiniKey token is not inserted, causing DocuSign Signature Appliance to turn itself off after two hours. Insert the correct license MiniKey and restart DocuSign Signature Appliance.
- A tamper event occurred, and the Tamper LED is blinking. Reset the Tamper mechanism from the console (refer to [Resetting the Tamper Mechanism](#)).
- DocuSign Signature Appliance failed to receive an IP address, and the Tamper LED is lit. Check the cable and DHCP server. Once the network problem is resolved, the LED turns off and DocuSign Signature Appliance begins working.
- The DocuSign Signature Appliance users OU was modified. Verify that the DocuSign Signature Appliance users OU was not modified, and it is the same as was entered during installation.

If none of the above is applicable, run the console and enter **1** from the main menu (refer to [Displaying Status](#)). Check the appliance information for the Service State parameter, as follows:

- If the Service State is **Running**, check for a network problem between DocuSign Signature Appliance and the clients.
- If the Service State is **Stopped**, restart DocuSign Signature Appliance and then recheck the Service State. If the Service State is still **Stopped**, contact ARX technical support (support@arx.com).
- If the Service State is neither **Running** nor **Stopped**, first check to see whether there is a networking problem (ping the IP address). If this is not the problem, contact ARX technical support (support@arx.com).

New Users Do Not Receive Certificates

Problem: When you add new users to the system, DocuSign Signature Appliance does not assign the users certificates.

Solution: Verify that the number of users does not exceed the license. To do this, check the number of users currently defined in the database and the number of users allowed by the license MiniKey token. Both numbers appear on the Display status page in the console (refer to [Displaying Status](#)).

If there are too many users defined in the Users OU, perform one of the following actions:

- Request a new license from ARX.
- Delete unnecessary users.
- Move some of the users to another OU.

Then perform Sync with Directory from the Administration MMC (refer to [Synchronizing DocuSign Signature Appliance with the](#) Directory Service).

If the number of users in the Users OU does not exceed the license, there may still be too many users defined in the database. Download the Event log. If this is the problem, the message `CoSign appliance reach license limit, please upgrade your CoSign license` appears. In this case, perform Sync with Active Directory from the Administration MMC.

Note: All users defined in the OU are counted toward the total number of users, including special users such as IUSR*, guest, etc.

Another cause may be that a user tried to log in immediately after being added to the system, before DocuSign Signature Appliance updated its database. In this case, the user should log off and then log in again.

Restore Appliance Fails

Problem: When you attempt to restore the appliance (refer to [Restoring the Appliance](#)), the operation fails immediately after inserting the backup MiniKey token. In this case, the failed to parse the backup header message appears in the Install log.

Solution: You may have inserted the wrong MiniKey token. Make sure that the MiniKey token you insert is the same MiniKey token that was used during the installation process.

If the correct MiniKey token was inserted and the Restore Appliance operation still fails due to MiniKey token hardware problems, try again using the second MiniKey token of the pair.

Backup Operation Fails

Problem: When attempting to back up the appliance using the `getbackup.exe` utility or the appliance management console, the backup process fails. The administrator has full administrative privileges on the MS Active Directory.

Cause 1: Administrative tasks can be performed only by a user who is himself a member of the DocuSign Signature Appliance administrators group (and not a member of a group that is member of the DocuSign Signature Appliance administrators group).

Solution 1: Check the name of the DocuSign Signature Appliance administrators group on the appliance console and make sure you are yourself a member of that group.

It is also possible to use the DocuSign Signature Appliance built-in administrator.

Cause 2: On the debug log you will see that the backup failed because it failed to copy the internal CA CRL file.

Solution 2: Perform a hardware restart.

Appendix A: Installation with Reduced Privileges

This appendix describes how to perform an installation in an Active Directory environment with reduced permissions.

Overview

When the appliance is installed in an Active Directory environment, you must login with an admin account and provide the installation wizard with both an admin account and a password, to enable both the appliance installation and the appliance operation in the MS Active Directory environment.

During installation, the administrative permissions enable the creation of new objects in the MS Active Directory and updating of existing objects. Access to the administrative account is limited to the installation phase, and is not required for the ongoing operation of DocuSign Signature Appliance.

DocuSign Signature Appliance installation is performed using the *Appliance Management* utility and is described in detail in *Chapter 3: Installing DocuSign Signature Appliance*.

There are cases where the appliance is installed in environments that do not have global administrative permissions, for example, a department of a big organization.

In this type of organization, there are several administrators for the organization's Active Directory, with each administrator responsible for maintaining a department that is defined as a specific OU (Organizational Unit) in the organization's Active Directory. These administrators have permissions only to manipulate objects in their department's OU, but do not have permission to update any objects outside that scope.

The client enables administrators with restricted permissions to install the appliance. Additional operations must be performed in addition to the actual installation, to provide a functionality similar to that of a privileged administrator performing an installation.

Note: In some cases, an installation with reduced privileges reduces the functionality of DocuSign Signature Appliance.

This appendix describes the differences between a regular installation and a installation with reduced privileges. It includes the following sections:

- [Regular Installation](#) – This section describes a regular appliance installation, with a focus on the Active Directory operations performed by the installation, and the functional purpose of each Active Directory operation.
- [Installation with Reduced Privileges](#) – This section describes the reduced appliance installation. It details the activities that must be carried out to enable the functionality provided by the regular installation procedure.

Note: You can switch to another administrative account if the current administrator fails to perform an operation which accesses the Domain. The failed administrator is prompted to supply an alternate administrator account.

This ability may resolve issues of reduced privileges.

For more information about this functionality, refer to [Permission Considerations](#).

Regular Installation

The following sections list all the operations carried out during appliance installation that require Enterprise admins or Domain admins permissions.

Creating a New Computer Account for the Appliance

The installation creates a new computer account for the appliance if an account does not yet exist. The installation also grants this account membership to *Cert publishers* and to *Pre-Windows 2000 Compatible Access*.

Joining the Appliance to MS Domain

In order to install DocuSign Signature Appliance in an Active Directory environment, the installation requires an administration machine joined to the domain and logged in with a user who is a member of the Enterprise admins and Domain admins groups.

Creating a Services Connection Point (SCP)

The installation creates an SCP object, which contains information (such as the IP address) that enables the Clients to connect to the appliance. This object is located in **Active Directory Sites and Services** → **Services** → Net **Services**.

The appliance computer account is granted read and write access rights so that the appliance can update SCP information.

User Synchronization

During normal operation, the appliance synchronizes periodically with the domain by querying for new, updated, or deleted user objects. It may also update the user certificate attribute of users for whom it had issued a certificate (refer to [Updating the userCertificate Attribute for Users](#) below). To enable proper synchronization of users, read access rights to the **Deleted Objects** container are granted to the appliance to enable querying the deleted user objects.

Updating the userCertificate Attribute for Users

DocuSign Signature Appliance does not update the certificate attribute of a user by default.

If you wish to update the certificate attribute of a user in Active Directory with the certificate content, you must grant write access rights to the **userCertificate** attribute for all users objects in the users OU. This is achieved by assigning the computer to the **Cert Publishers** group as part of the installation procedure. To complete the process, you must change the value of the *User Certificate Publishing* system parameter to True and perform a soft restart of the appliance.

CA Root Certificate Information

AIA (Authority Information Access) and CA objects that contain the published Certificate Authority root certificate are updated by the appliance during installation. This information automatically updates all machines in the domain, thereby providing proper signature verification. The objects are located in **Active Directory Sites and Services** → **Services** → **Public Key Services** → **AIA**, and **Active Directory Sites and Services** → **Services** → **Public Key Services** → **CA**.

Read and write access rights are granted to the appliance computer account so that the appliance can publish and update CA objects.

CA CDP (Certificate Distribution Point)

The CA CDP (CRL Distribution Point) contains the updated the published CRL (Certificate Revocation List). This object is located in **Active Directory Sites and Services → Services → Public Key Services → CDP**.

Read and write access rights are granted to the appliance computer account so that the appliance can publish and update new CRLs.

Installation with Reduced Privileges

During the installation procedure, both the login administrative user and the provided administrator account can have fewer privileges than domain admins and enterprise admins. However, at the end of the data collection stage, a warning appears listing the operations that failed during the creation of Active Directory objects, due to insufficient privileges. To restore the reduced functionality, perform the following steps, as described in the following sections:

- Add the computer to the domain as a preliminary action to be taken before installing with reduced privileges.
- Install DocuSign Signature Appliance in a reduced-privileges environment.
- Complement the installation with the DocuSign Signature Appliance capabilities that were described in [Regular Installation](#).

Preliminary Action – Adding the Computer to the Domain

Prior to running the installation, add the computer to the domain, as follows:

- Add a computer account to the Active Directory and set the name of the user who can join this computer to the domain. The computer name field should be set according to the serial number (refer to [Displaying Status](#)). For example, **CSN00041**.
- Set the *user* or *group* to a user or group that can join this computer to the domain.

Note: The admin user provided during installation should be the above user or a user who is a member of the assigned group.

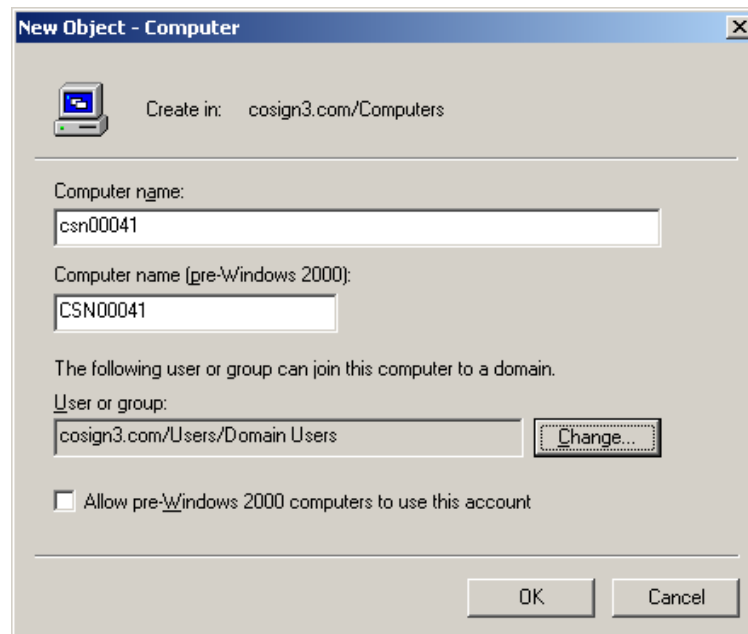


Figure 93 Adding the Computer to the Domain

Installing in a Reduced Privileges Environment

After adding the computer to the domain, activate the Appliance Management and install the appliance according to the following guidelines:

- In the *User Setup* window provide the username and password for an account with permission to join the machine to the domain.
- In the *Directory Setup* window set the **CoSign Container** field with the full OU (or container) path of the computer account that was generated in the preliminary stage.
- Click **Finish**. A message appears listing the operations that failed during the creation of Active Directory objects.

Note: The list of failed operations depends on the extent of the user's privileges.

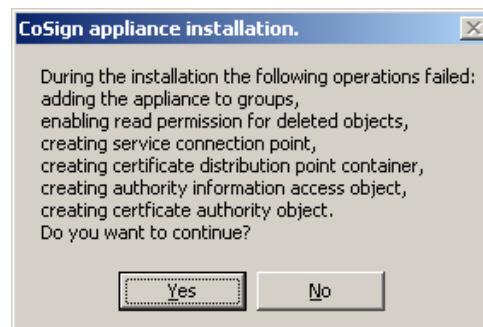


Figure 94 Installation Failure Message

- Click **Yes** to continue with the installation.

The installation will try to create/update objects in the Active Directory. Any object listed in the above warning message will not be generated or updated.

Complementing the Installation with Missing Capabilities

Once installation with reduced privileges is complete, you can complement it with the missing capabilities. This section describes how to restore the capabilities after installing with reduced privileges.

Note: After you update any of the objects in the Active Directory, restart the appliance.

Joining the Appliance to the MS Domain

For DocuSign Signature Appliance to work, it is mandatory that the user specified in the *User Setup* window has permission to join the appliance to the Domain.

Administering after the installation

To administrate DocuSign Signature Appliance after the installation, use the *Configuration Utility* (described in [Chapter 8: Configuration Utility](#)) to set the value of **Admin** → **Administrator's Group Name** to the administrators groups of the division. For example, set the value to be *Division Admin Users*. Alternatively, you can administrate DocuSign Signature Appliance using the built-in administrator.

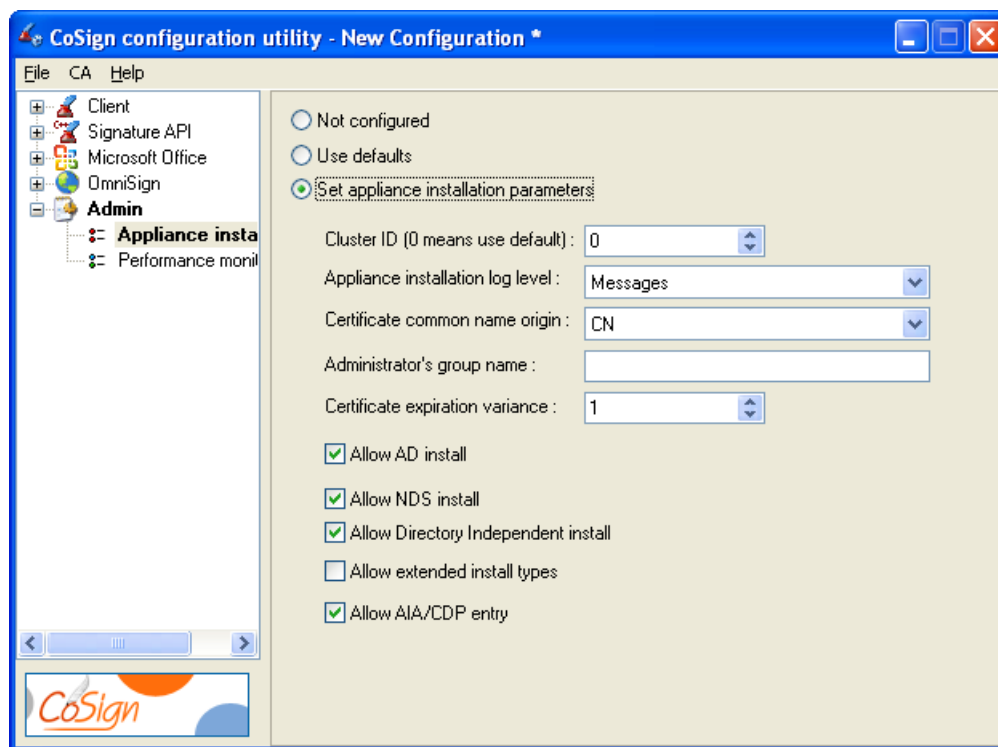


Figure 95 Setting the Administrator's Group Name

Creating a Services Connection Point (SCP)

Failure to create an SCP prevents the appliance from publishing its binding information, thus preventing clients from locating the appliance. Once the computer is granted access rights to the SCP, this functionality is enabled.

If it is a problem to enable such access, it is still possible to manually set this information through the Client Configuration utility (refer to [Distributing DocuSign Signature Appliance Information through the SCP](#)). However, this option is limited for the following reasons:

- The client is never updated with the current status of the appliance activity. This causes long delays when attempting to connect to an inactive appliance.
- Any update of information, such as the appliance's IP address, involves a manual update of all clients.

User Synchronization

Failure to set read access rights to the **Deleted Objects** container causes synchronization problems of deleted users from the Active Directory. Since deleted users are not recorded as deleted, you can reach the license limitation when the actual number of users is well under the limitation.

You can take the following action:

- After any deletion of users from the Active Directory, perform a manual full synchronization of the appliance (refer to [Synchronizing DocuSign Signature Appliance with the Directory Service](#)).

Updating the userCertificate Attribute for Users

Failure to assign the computer as a member of the *Cert Publishers* group causes problems in setting the user's certificate in the Active Directory. You can take any of the following actions:

- Manually assign the computer as a member of the *Cert Publishers* group.
- Grant the computer write access to the relevant users.
- Publish the user certificate manually, or refrain from publishing users' certificates.

Note that DocuSign Signature Appliance does not update the certificate attribute of the user by default.

CA Root Certificate Information

Failure to create the AIA prevents the server from automatically publishing its ROOT certificate. Since the ROOT CA must be part of the trusted Certificate Authorities, you can take any of the following actions:

- Distribute the root certificate manually or automatically using administrator tools. Refer to [Chapter 4: Deploying the DocuSign Signature Appliance Client](#) for more information.
- During the installation of the appliance, you can define a different AIA location (such as an HTTP location), or not specify any AIA location.
- Create the AIA object in the Active Directory after the installation, and publish the root certificate manually.

CA CDP (Certificate Distribution Point)

Failure to create a CDP prevents the appliance from publishing its updated CRL. This may cause signature or verification problems or delays since the updated CRL is not located in its designated location. You can take any of the following actions:

- The CRL expiration time can be set to expire several years in the future. By setting the CRL once in the CDP, all applications that require CRLs will work properly.
- Distribute the CRL manually or automatically using administrator tools.

- During appliance installation, you can define a different CDP location (such as an HTTP based location), or specify that the CRL is not required.
- Create this object in the Active Directory after the installation, and then either publish the CRL manually, or grant the appliance the proper rights to update this object.

Appendix B: Centralized Client Installation

The client can be centrally deployed in any environment, using various methods. Some of the methods can be based on Microsoft Active Directory or alternative Microsoft tools or on third party tools. It is essential to use such utilities in the case of large deployments.

This appendix describes one of the ways of deploying the client in a large scale organization using Microsoft SCCM (System Center Configuration Management).

Automatic Client Deployment using Microsoft SCCM

Microsoft SCCM (System Center Configuration Management) enables you to automatically perform remote software installations. Using this feature, you can install the client on all relevant workstations without user intervention, resulting in a smooth deployment of the system in a large-scale organization.

For more information refer to the Microsoft documentation at <http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2-configuration-manager/>.

Note: The following description is based on SCCM version 2007. The flow of operations in SCCM 2012 is similar.

Automatic deployment in a Microsoft Active Directory can be performed as follows:

- Place the contents of the CoSign CD in a specific shared location in the domain, such as a shared disk drive of the domain server or any other Microsoft-based file server in the domain.
- Define a Task Sequence in Microsoft SCCM. When the task sequence is advertised, the relevant workstations will install the client software.
For more information, refer to [Defining and Advertising a Client Task Sequence](#).

Installation Components

The following table lists the components of the Client installation, and their location in the CoSign CD. These files are used to define which Client software packages SCCM will install. Some of the files differ depending on the intended operating system (32-bit or 64-bit).

Table 2 Client Installation Components

Installation Files for 32-bit Operating Systems	Installation Files for 64-bit Operating Systems	Location
ARX CoSign Client.msi	ARX CoSign Client64.msi	CDRom\MSI
ARX CryptoKit Basic.msi	ARX CryptoKit Basic64.msi	CDRom\CryptoKit
ARX Signature API.msi	ARX Signature API64.msi	CDRom\MSI
ARX CoSign Printer.exe(Optional)	ARX CoSign Printer.exe(Optional)	CDRom\MSI
ARX Office Signatures.msi (Optional)	ARX Office Signatures64.msi (Optional)	CDRom\MSI

Defining and Advertising a Client Task Sequence

This section describes in detail how to define a Microsoft SCCM Task Sequence for client installation, and how to advertise the Task Sequence so it performs automatic mass client installation in large scale client deployments.

Step 1: Define Packages

To define a packages:

- Open the SCCM Configuration Manager Console.
- Navigate to **Computer Management > Software Distribution > Packages**.
- Select **New > Package From Definition** to add as software packages each of the following software components (.MSI files) that you had placed in the shared location:
 - ARX CoSign Client.msi
 - ARX Cryptokit Basic.msi
 - ARX Signature API.msi
 - ARX Office Signatures.msi (if required)

The full list of packages will look similar to the following:

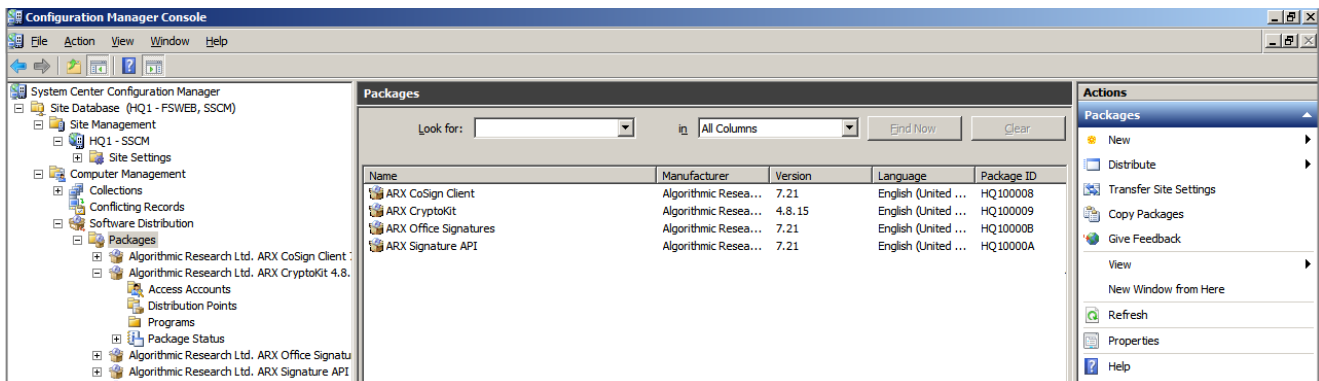


Figure 96 Defining the Packages

Step 2: Create a Task Sequence

To create a task sequence:

- Navigate to **Computer Management > Operating System Deployment > Task Sequences**.

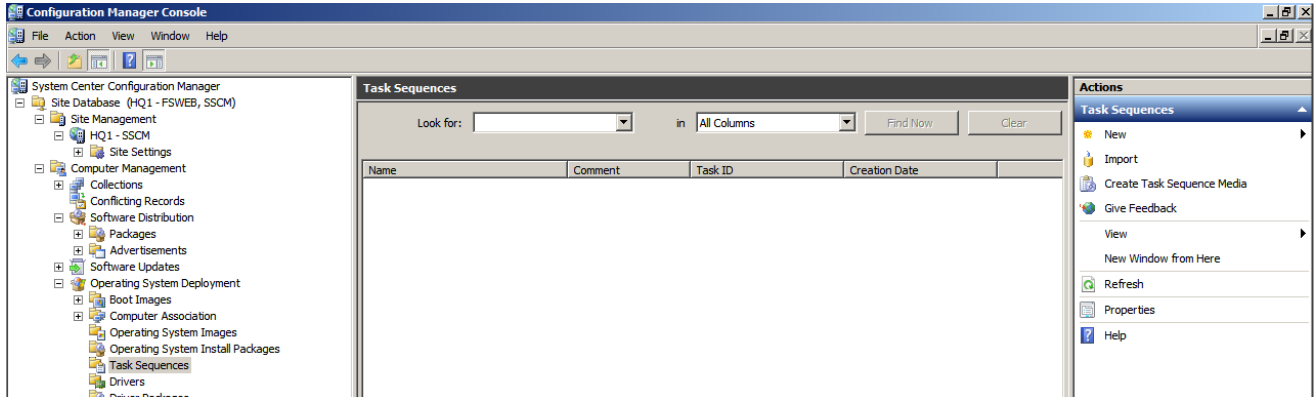


Figure 97 Task Sequences Window

- Select **New > New custom task Sequence**. The New Task Sequence Wizard is launched.

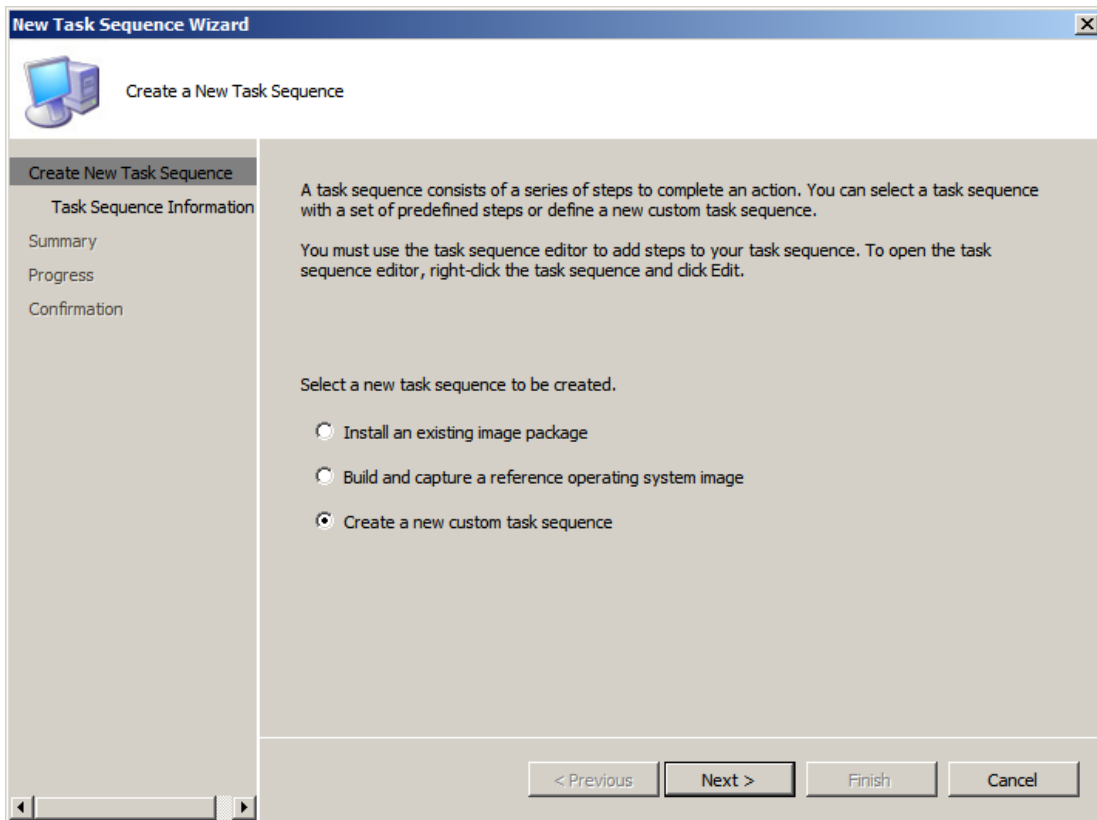


Figure 98 New Task Sequence Wizard

- Select **Create a new customTask Sequence**.
- Give the new task sequence a name. It is recommended to give it the same name as the installed Client version.

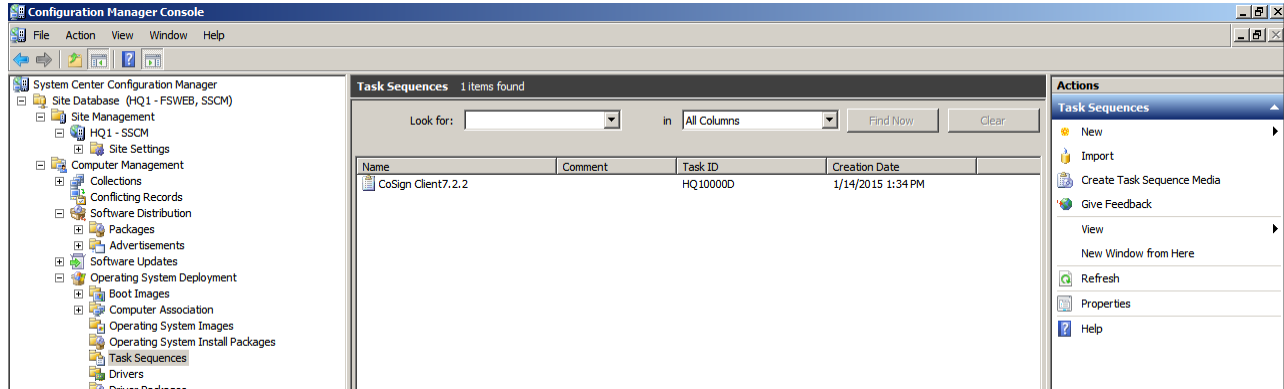


Figure 99 Name of Task Sequence

- Right-click the newly created Task Sequence and select **Edit**. The Task Sequence Editor window appears.

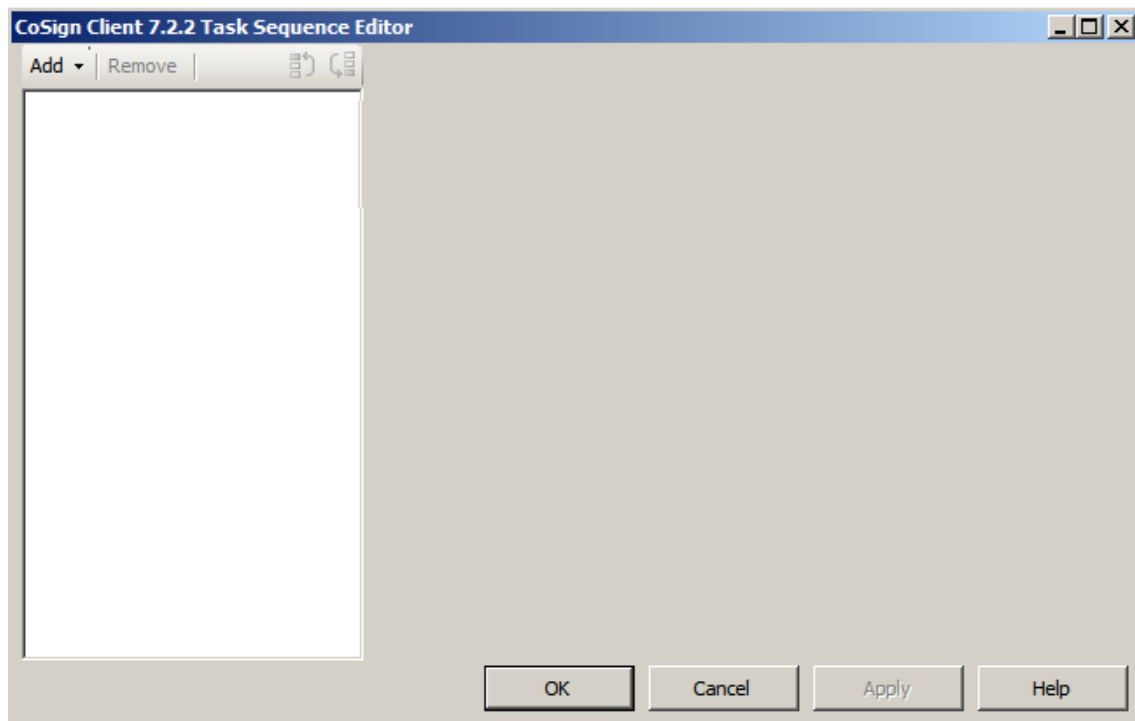


Figure 100 Task Sequence Editor window

- Install the Client as follows:
 - Select **Add > General > Install Software**.

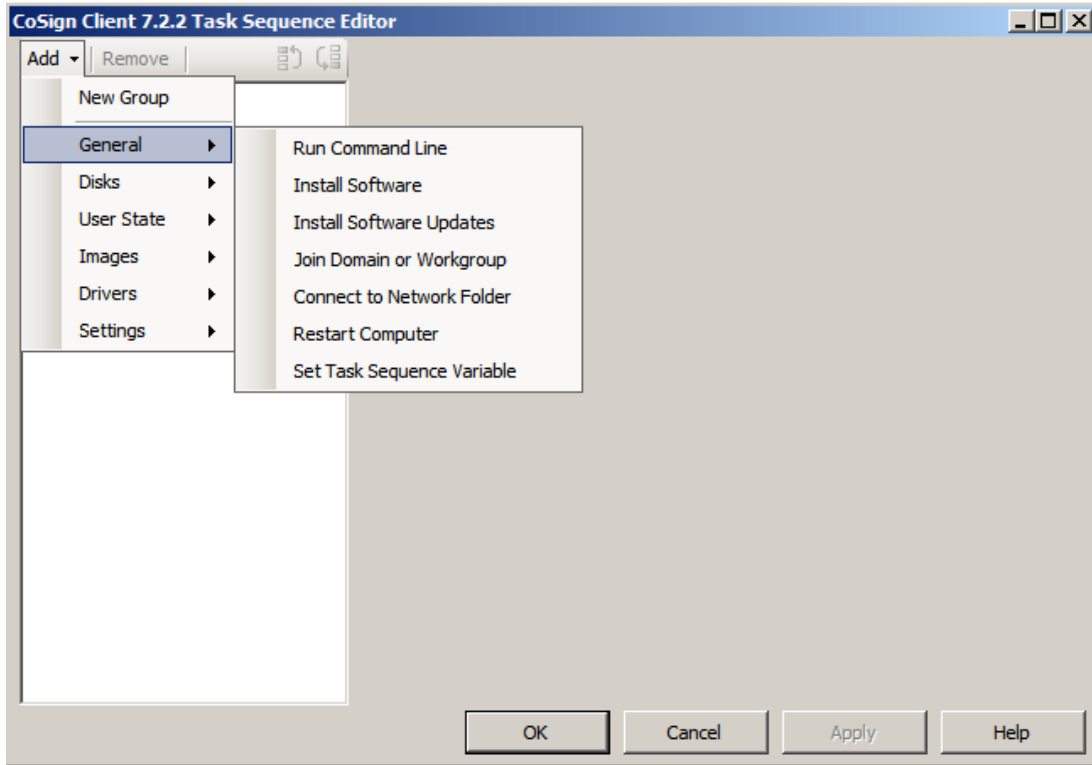


Figure 101 Selecting to Install Software

- In the **Name** field, enter a meaningful name for the software.
- Click **Browse** to select the relevant package.
- Verify that **Per-system unattended** is selected in the **Program** field.

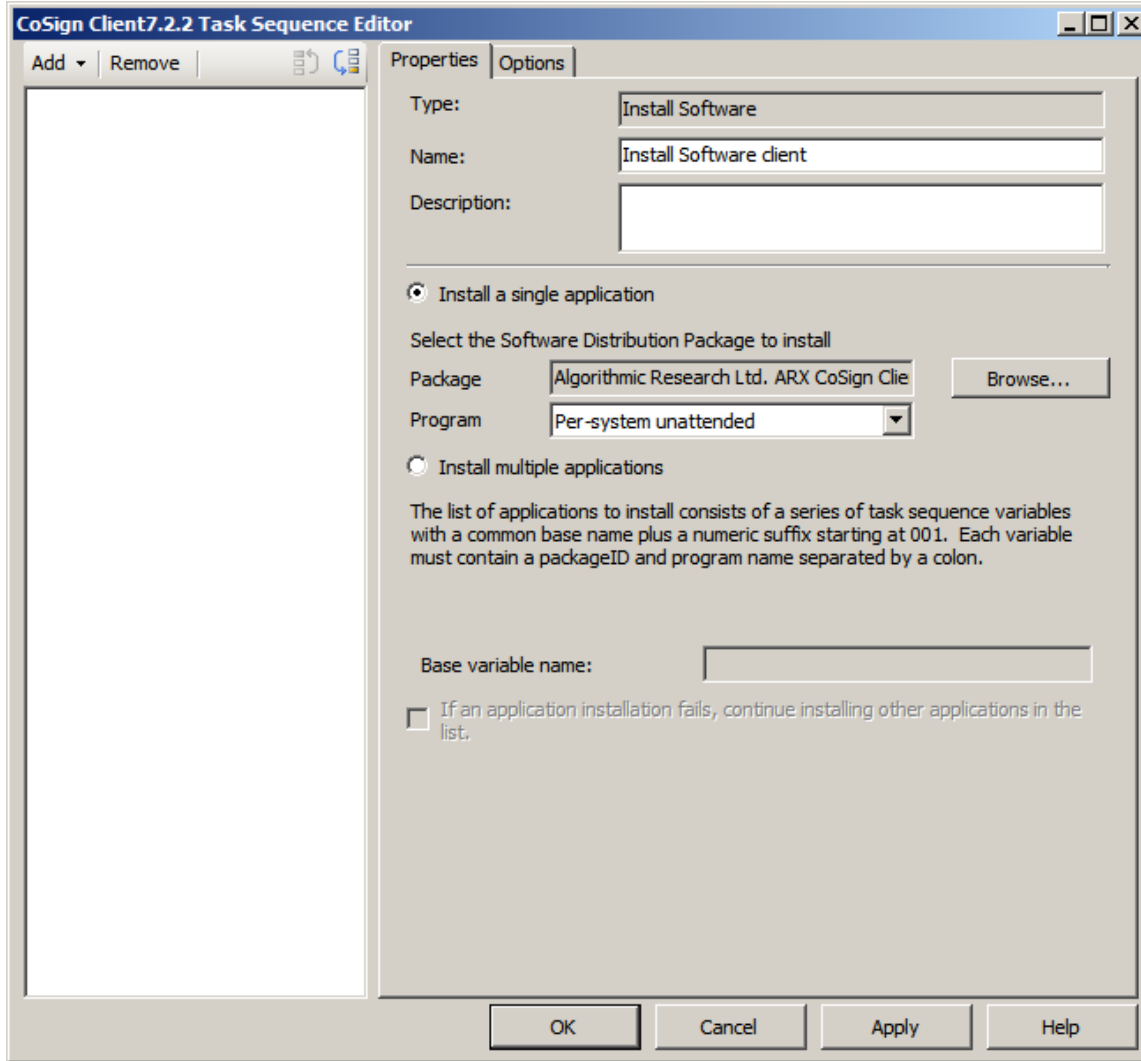


Figure 102 Installing a Package as Software

- Click **Apply**.
- Install CryptoKit as follows:
 - Navigate to **Add > General > Run Command Line**.

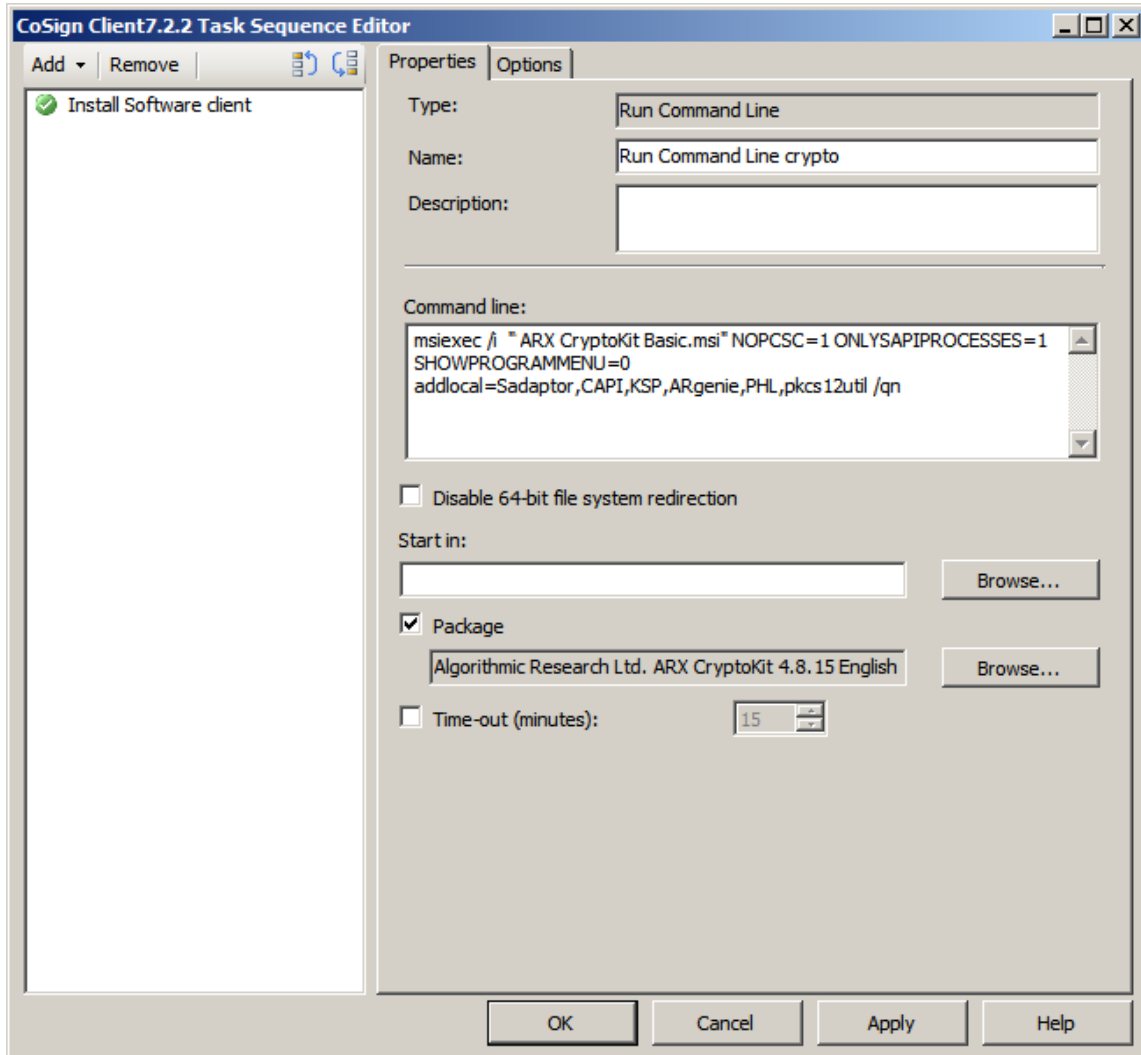


Figure 103 Installing CryptoKit

- In the **Name** field, enter a meaningful name for the software.
- Click **Browse** to select the relevant package.
- In the **Command line** field enter the following text:

```
msiexec /i "ARX CryptoKit Basic.msi" NOPCSC=1 ONLYSAPIPROCESSES=1
SHOWPROGRAMMENU=0 addlocal=Sadaptor,CAPI,KSP,ARgenie,PHL,pkcs12util /qn
```
- Click **apply**.
- Install the DocuSign Signature Appliance Signature API as follows:
 - Select **Add > General > Install Software**.
 - In the **Name** field, enter a meaningful name for the software.
 - Click **Browse** to select the relevant package.
 - Verify that **Per-system unattended** is selected in the **Program** field.
 - Click **Apply**.
- Optionally install the Office Signatures as follows:

- Select **Add > General > Install Software**.
 - In the **Name** field, enter a meaningful name for the software.
 - Click **Browse** to select the relevant package.
 - Verify that **Per-system unattended** is selected in the **Program** field.
 - Click **Apply**.
- Optionally install the Printer as follows
 - Navigate to **Add > General > Run Command Line**.

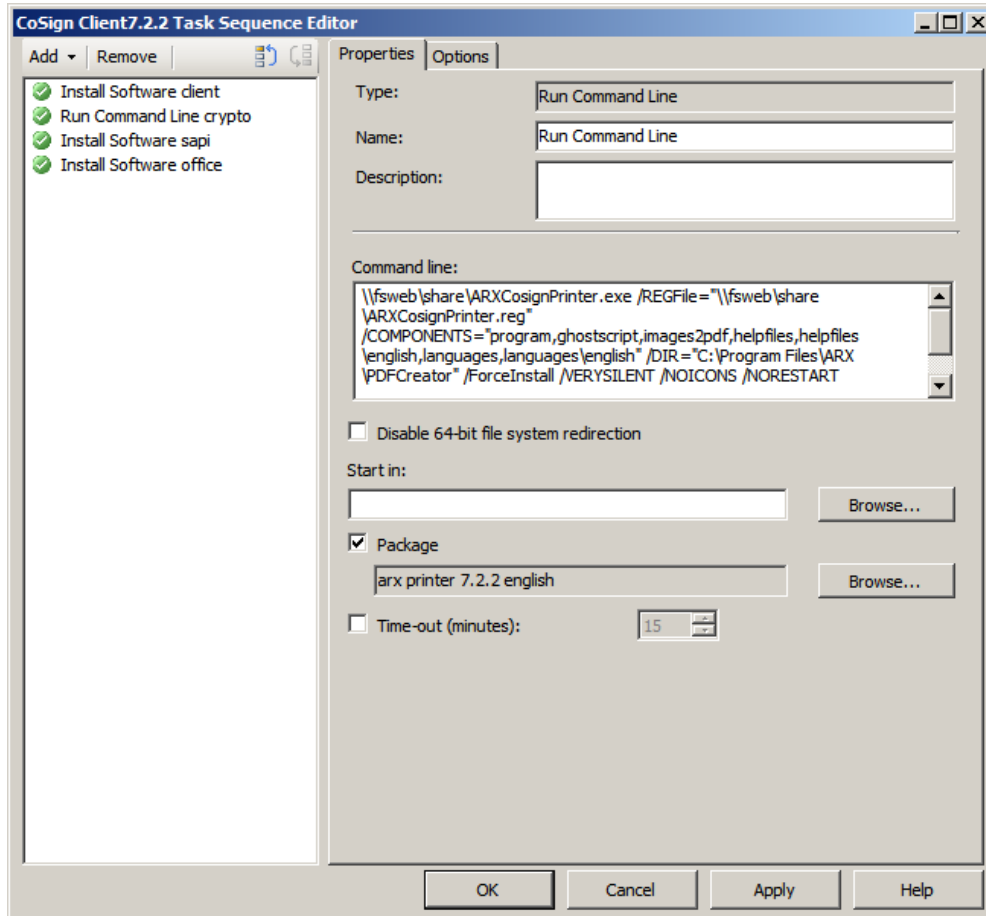


Figure 104 Installing the Printer

- In the **Name** field, enter a meaningful name for the software.
- Click **Browse** to select the relevant package.
- In the **Command line** field enter the following text:


```
\\{share}\ARXCosignPrinter.exe /REGFile="\\{share}\ARXCosignPrinter.reg"
/COMPONENTS="program,ghostscript,images2pdf,helpfiles,helpfiles\english,languages,languages
\english" /DIR="C:\Program Files\ARX\PDFCreator" /ForceInstall /VERYSILENT /NOICONS
/NORESTART /Printrname="ARX CoSign" /LANG=english /TASKS=
/RESTARTEXITCODE=999
```

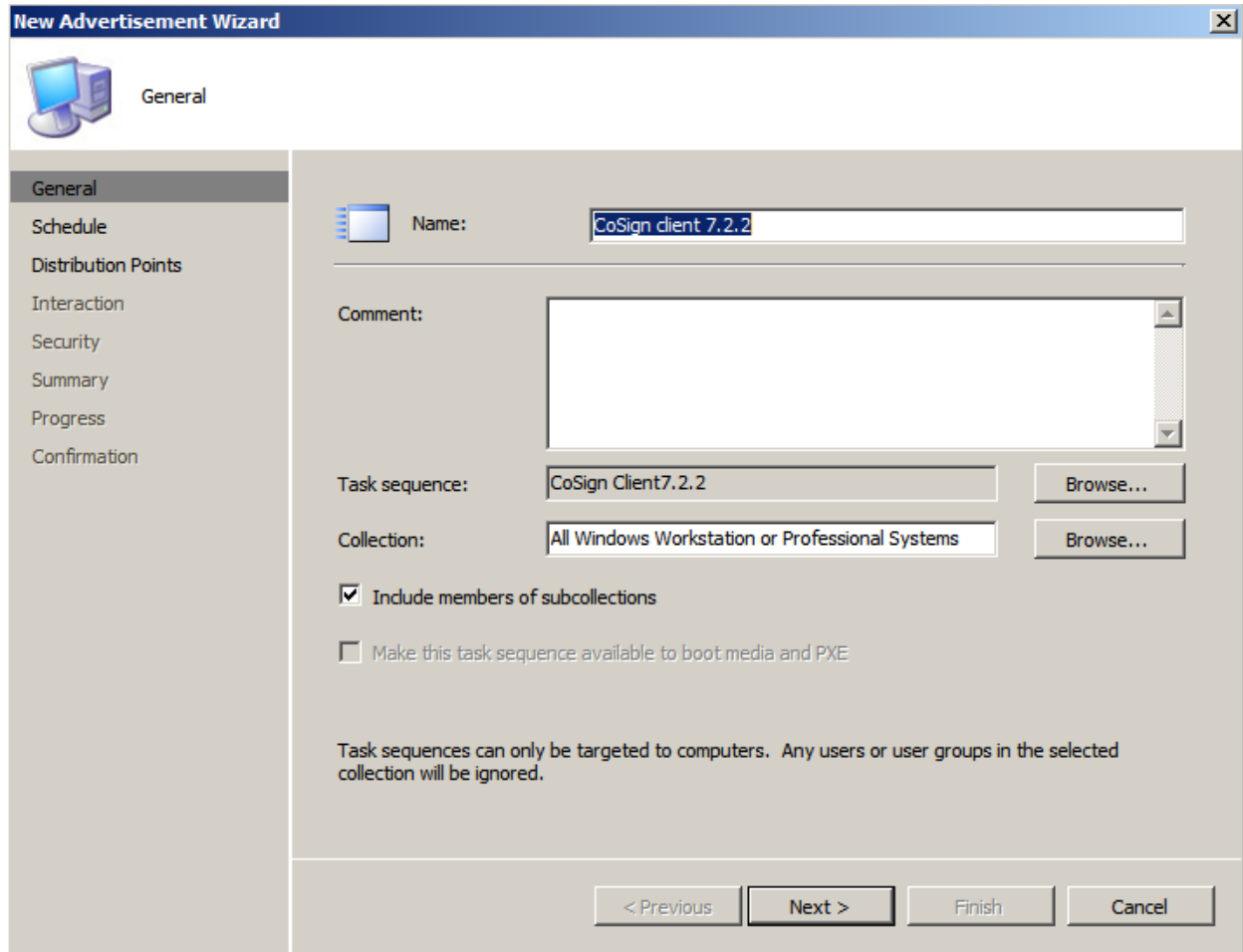
 where **{share}** is the location of the shared disk.
- Click **Apply**.

- Click **OK**.

Step 3 – Advertise the Task Sequence

To advertise the task sequence:

- Navigate to **Computer Management > Software Distribution > Advertisements**.
- Select **Advertise Task Sequence**. The New Advertisement Wizard is launched.



The screenshot shows the 'New Advertisement Wizard' dialog box with the 'General' tab selected. The 'Name' field contains 'CoSign client 7.2.2'. The 'Task sequence' field contains 'CoSign Client7.2.2' and the 'Collection' field contains 'All Windows Workstation or Professional Systems'. There are 'Browse...' buttons next to both the 'Task sequence' and 'Collection' fields. The 'Include members of subcollections' checkbox is checked, and the 'Make this task sequence available to boot media and PXE' checkbox is unchecked. A note at the bottom states: 'Task sequences can only be targeted to computers. Any users or user groups in the selected collection will be ignored.' Navigation buttons at the bottom include '< Previous', 'Next >', 'Finish', and 'Cancel'.

Figure 105 New Advertisement Wizard

- Give the new task advertisement a name. It is recommended to give it the same name as the task.
- Click **Browse** adjacent to the **Task Sequence** field to select the task sequence
- Click **Browse** adjacent to the **Collection** field to specify on which workstations to install the packages in the task sequence.
- Click **Next**, and in the Schedule window set the date and time of the installation.
- Click **Next** in all subsequent wizard windows, and click **Finish** in the final window.

Index

- :setting debug level, 128
- Accepting Relying Parties Tickets, 136
- Accessing, troubleshooting, 206
- Account Activation, 86
- Activating a user, 21
- Active Directory. *See* Microsoft Active Directory
- Add Certificate to CRL, 122
- Add Digital Signature checkbox disabled, 205
- Additional Radius IPs (CC Mode), 134
- ADFS, 23
- Administration MMC
 - backing up database, 101
 - capabilities, 100
 - changing system parameters, 116
 - downloading log files, 107
 - high availability options, 108
 - managing data replication, 183
 - monitoring appliance performance, 113
 - obtaining a new license, 114
 - operations fail, troubleshooting, 206
 - overview, 99
 - renewing subordinate CA certificate, 110
 - restarting DocuSign Signature Appliance, 108
 - restarting DocuSign Signature Appliance services, 108
 - restoring the appliance in a Directory Independent environment, 139
 - restoring the appliance in Active Directory, 138
 - restoring the appliance in LDAP environment, 139
 - restoring the appliance, overview, 138
 - starting, 99
 - synchronizing DocuSign Signature Appliance with the directory service, 104
 - system parameters, troubleshooting, 205
 - uploading software updates, 102
 - uploading SSL certificate, 112
 - usage prerequisites, 99
- administrative client
 - installation requirements, 28
 - installing, 28
 - uninstalling, 29
- Administrative client
 - installation overview, 27
- Administrative problems, troubleshooting, 205
- AIA Location Settings, 121
- AIA Publication Location, 121
- Allow Get Backup Anonymously, 130
- Alternate appliance
 - data replication management, 183
 - installing, 178
 - installing hardware, 179
 - installing software, 179
 - managing, 183
 - re-initializing, 184
 - resubscribing, 188
 - setting as primary appliance, 185
 - unsubscribing, 185
 - viewing replication status, 184
- Alternate DocuSign Signature Appliance
 - overview, 177
- Alternate Extended Auth Mode, 132
- Alternate Radius Server IP Address, 133
- Alternate Radius Server port, 134
- Appliance
 - configuring installation parameters, 199
 - configuring performance monitoring parameters, 200
 - configuring the signing operation using the Configuration Utility, 198
 - connecting CoSign Central Enterprise, 37
 - connecting CoSign Central FIPS HW v7.0, 34
 - connecting DocuSign Signature Appliance Central FIPS HW v8.0, 30
 - CoSign Central Enterprise back panel, 38
 - CoSign Central Enterprise front panel, 38
 - CoSign Central FIPS HW v7.0 front panel, 34
 - CoSign Central FIPS HW v8.0 back panel, 35
 - DocuSign Signature Appliance Central FIPS HW v8.0 back panel, 31
 - DocuSign Signature Appliance Central FIPS HW v8.0 front panel, 30
 - managing, 99
 - not in factory settings mode, error message, 202
 - restarting appliance, 108
 - restarting services, 108
 - restore operation fails, 207
 - restoring in Active Directory, 138
 - restoring in Directory Independent environment, 139
 - restoring in LDAP environment, 139
 - restoring, overview, 138
 - synchronizing with directory service, 104
 - viewing information in console for HW before v7.0, 159
 - viewing information in web-based Console, 171
- Appliance Administrator Group, 117
- appliances
 - monitoring performance, 113
 - obtaining a new license, 114
- Appliances
 - software installation, 40
- Applications that work with DocuSign Signature Appliance, 10

- Architecture, 15
- Authenticating
 - data, requirements, 9
 - users in DocuSign Signature Appliance, 16
- Authentication methods, 16
- Authentication, extended authentication mechanisms, 16, 97
- Automatic Deletion of Users, 117
- Automatic deployment of client
 - in Active Directory, 216
 - overview, 216
- Back panel
 - CoSign Central Enterprise, 38
 - CoSign Central FIPS HW v8.0, 35
 - DocuSign Signature Appliance Central FIPS HW v8.0, 31
- Backing up the database, 101
- Backup
 - backup fails, troubleshooting, 207
 - command line utility, 152
 - operation, 101
 - restoring appliance from, 138
- Batch scripts, 151
- Biometric Authentication, 131
- Biometric Authentication Window, 132
- Biometric Shared Secret, 132
- Built-in Admin, 119
- CA Cert Hash Algorithm, 122
- Case Sensitive Username, 130
- CD
 - installation files, 77
 - uninstalling DocuSign Signature Appliance software, 80
- CDP location settings, 121
- Central Enterprise
 - configuring console terminal, 157
 - resetting tamper mechanism in Console for HW before v7.0, 162
- Central storage of keys, 16
- Centralized installation of client, 216
- Certificate Common Name, 121
- Certificate Expiration Variance, 120
- Certificate Issuer Name, 133
- Certificate Refresh Timer, 120
- Certificate Refresh Window, 120
- Certificate Revocation List (CRL)
 - CRL publishing frequency, 120
 - downloading to a file, 192
- Certificate Validity Period, 122
- Certificates
 - automatic external CA mode, 19
 - certificate validity period, 122
 - clearing CA files, 106
 - CoSign Central FIPS HW v7.0 certificates compliance, 36
 - creating for each computer, 118
 - DocuSign Signature Appliance Central FIPS HW v8.0 certificates compliance, 33
 - expiration variance, 120
 - groups, 118
 - internal CA, installing, 65
 - manual external CA mode, 18
 - none in store, 205
 - parameters, setting, 120
 - publishing, 118
 - refresh timer, 120
 - refresh window, 120
 - refreshing, 106
 - ROOT, adding to trusted CA list, 97
 - ROOT, installing, 96
 - setting common name, 121
 - troubleshooting, 206
- Client
 - client components installation screen, 79
 - deployment
 - deployment options, 75
 - introduction, 75
 - on end-user machine, 76
 - on terminal server, 76
 - on Web server, 76
 - overview, 75
 - installing, 76, *See* Client installation
 - installing centrally, 216
 - setting security parameters, 124
 - software components, 77
 - supported operating systems, 75
 - troubleshooting, 204
 - uninstalling, 80
- Client installation
 - automatic centralized deployment, 80
 - centralized installation, 216
 - client MSI files, 216
 - installing from CD, 78
 - overview, 76
 - prerequisites, 78
 - selecting the language, 79
- Clients Inactivity Timeout, 128
- Cloud Monitoring, 131
- Cloud Site ID, 131
- Command line utilities
 - GetBackup, 152
 - GetEvt, 153
 - Groups, 155
 - installing, 151
 - overview, 151
 - RestartServer.exe, 154
 - SetSCP, 155
 - Switch2Prim, 154
- Common Criteria EAL4+, 19
 - certificate enrollment, 21
 - DocuSign Signature Appliance installation procedure, 63
 - Radius server, 19

- signature key generation, 21
- user activation, 21
- Common Criteria Mode, 130
 - Radius callback list, 134
- Common Criteria Type, 130
- Comodo external CA, setting, 70
- Configuration Utility
 - Admin mode
 - configuration file operations, 195
 - creating a configuration file, 195
 - exporting to a configuration file, 195
 - exporting to a group policy, 196
 - group policies operations, 196
 - opening a configuration file, 195
 - opening a group policy, 196
 - usage, 194
 - CA menu, 192
 - distributing a client configuration
 - manual distribution, 197
 - overview, 196
 - via configuration files, 197
 - via distributing software, 198
 - via group policy, 198
 - via login scripts, 198
 - downloading the ROOT certificate, 192
 - editing parameters, 190
 - End User mode, 196
 - File menu, Admin mode, 191
 - generating an installation report, 193
 - Help menu, 192
 - installing the ROOT certificate, 192
 - introduction, 189
 - menus, 191
 - modes of operation, 189
 - overview, 189
 - running, 189
 - setting appliance configuration
 - appliance installation parameters, 199
 - overview, 198
 - performance monitoring parameters, 200
 - using, 189
- Configuring
 - console terminal, 157
- Configuring, using the Configuration Utility, 189
- Console
 - accessing, 157
 - configuring the terminal, 157
 - error messages, 204
 - troubleshooting, 204
 - USB to serial adaptor, 158
- Console for HW before v7.0
 - enabling DHCP, 161
 - messages, 159
 - overview, 157
 - resetting tamper, 162
 - restoring factory settings, 163
 - setting CoSign time, 164
 - setting static IP address, 161
 - shutting down CoSign, 164
 - updating display, 159
 - using, 159
 - viewing information, 159
- Console, web-based
 - enabling DHCP, 167
 - overview, 157
 - resetting tamper, 170
 - restarting appliance, 170
 - restoring factory settings, 170
 - setting appliance IP address, 167
 - setting time, 167
 - shutting down DocuSign Signature Appliance, 169
 - touch screen, using, 174
 - using, 165
 - viewing information, 171
- Contact Name, 135
- Control Panel
 - Administrator actions, 84
 - in a Directory Independent environment, 85
 - menu bar options, 84
 - overview, 82
 - User actions, 83
- CORS domain for REST API, 130
- CoSign
 - shutting down in Console for HW before v7.0, 164
 - time and date, setting in Console for HW before v7.0, 164
- CoSign appliances HW v7.0
 - installing, 34
- CoSign Central Enterprise
 - back panel, 38
 - front panel, 38
 - hardware installation, 37
 - physical dimensions, 38
- CoSign Central FIPS HW v7.0
 - front panel, 34
- CoSign Central FIPS HW v7.0
 - hardware v8.0 installation, 34
- CoSign Central FIPS HW v7.0
 - environmental conditions, 36
- CoSign Central FIPS HW v7.0
 - certificates compliance, 36
- CoSign Central FIPS HW v8.0
 - back panel, 35
- CoSign verifier
 - installing, 97
 - validating signatures, 97
- CPS Object ID, 122
- CPS URI, 122
- Create Computer Keys, 118
- Create Group Keys, 118
- Create User Key Mode, 119
- CRL Publication Location, 121
- CRL Publishing Frequency, 120
- CRL Retrieval, 133

- CRL Validity Period, 121
 - Data authentication systems, 9
 - Data flow in DocuSign Signature Appliance, 15
 - Data replication management
 - accessing, 183
 - re-initializing an alternate appliance, 184
 - unsubscribing an alternate appliance, 185
 - viewing replication status, 184
 - Database, backing up, 101
 - Date, setting in , web-based Console, 167
 - Date, setting in Console for HW before v7.0, 164
 - Debug
 - level, 128
 - log, downloading, 107
 - Debug Level, 128
 - Default Radius password length, 133
 - Delete expired users by window, 123
 - Deleting graphical signature, 92
 - DHCP
 - enabling in Console for HW before v7.0, 161
 - enabling in web-based Console, 167
 - Digital signatures, prompting for signature, 124
 - Directory Independent environment
 - activating the account, 86
 - changing the password, 86
 - Directory Independent Users Management utility, 140
 - installing DocuSign Signature Appliance software, 58
 - overview, 17
 - password policy, 126
 - restoring appliance, 140
 - using the Control Panel, 85
 - Directory Server Search Base, 118
 - Directory Synchronization Timer, 117
 - Disabled checkbox, troubleshooting, 205
 - Disabling digital signatures, 205
 - DocuSign Signature Appliance
 - applications that work with DocuSign Signature Appliance, 10
 - architecture, 15
 - components, 11
 - data flow, 15
 - documentation, 12
 - end user platforms, 12
 - environments supported by DocuSign Signature Appliance, 10
 - installation, 27
 - installing client directly from CD, 77
 - installing signature capture device, 88
 - installing with reduced privileges, 209
 - managing graphical signatures, 89
 - shutting down in web-based Console, 169
 - turnkey solution, 17
 - uninstalling client, 80
 - using Graphical Signature Management application, 87
 - DocuSign Signature Appliance appliances
 - DocuSign Signature Appliance Central Enterprise, 12
 - overview, 12
 - DocuSign Signature Appliance Central Enterprise
 - description, 12
 - environmental conditions, 40
 - physical dimensions, 39
 - DocuSign Signature Appliance Central FIPS
 - description, 12
 - DocuSign Signature Appliance Central FIPS HW v8.0
 - front panel, 30
 - DocuSign Signature Appliance Central FIPS HW v8.0 hardware v8.0 installation, 30
 - DocuSign Signature Appliance Central FIPS HW v8.0 back panel, 31
 - DocuSign Signature Appliance Central FIPS HW v8.0 physical dimensions, 31
 - DocuSign Signature Appliance Central FIPS HW v8.0 environmental conditions, 32
 - DocuSign Signature Appliance Central FIPS HW v8.0 certificates compliance, 33
 - DocuSign Signature Appliance Central FIPS HW v8.0 physical dimensions, 35
- DocuSign Signature Appliances
 - DocuSign Signature Appliance Central FIPS, 12
 - DocuSign Signature Appliances HW v8.0
 - installing, 29
 - Downloading log files, 107
 - Email From Address, 126
 - Email notifications
 - configuring, 68
 - mail server name parameter, 125
 - Enable Automatic User Logon, 124
 - Enable the Radius AD Attribute, 134
 - Enable User Counters, 125
 - End-user machine, deploying client on, 76
 - Enforce CRL Validation, 133
 - Enforce FIPS Approved Algorithms, 130
 - Enhanced Key Usage Enabled, 123
 - Enhanced Key Usage Mask, 123
 - Enrolling users, 15
 - Environmental conditions
 - CoSign Central FIPS, 36
 - DocuSign Signature Appliance Central Enterprise, 40
 - DocuSign Signature Appliance Central FIPS, 32
 - Environments supported by DocuSign Signature Appliance, 10
 - Error messages
 - appliance not in factory settings mode, 202
 - failed error 51, 201
 - failed error 52, 201
 - failed error 54, 201
 - IP address is invalid, 201
 - licensing issues, 204

- the snapshot for this publication has become obsolete, 203
- Event log
 - command line utility, 153
 - downloading, 107
 - enabling user counters, 125
 - reporting client application name, 125
 - reporting signature events, 125
 - storage period, 125
- Event log storage period, 125
- Expiration date of license, 161, 173
- Expiration variance, certificates, 120
- Expired user action, 122
- Extended Authentication
 - devices, 97
 - parameters, setting, 131
 - supported modes, 97
- Extended Authentication Method, 131
- External CA Password, 123
- External CA User Name, 123
- External CA, automated mode
 - available WWV CAs, 70
 - Comodo, 70
 - overview, 19
 - SSL proxy settings, 68
 - synchronizing with DocuSign Signature Appliance, 105
- External CA, manual mode, 69
- Extractable Keys, 119
- Factory settings mode error message, 202
- Factory settings, restoring in Console for HW before v7.0, 163
- Factory settings, restoring in web-based Console, 170
- Failed
 - installation, 202
 - operations in Administration MMC, 206
- FIPS box HW v7.0, certificates' compliance, 36
- FIPS box HW v8.0, certificates' compliance, 33
- Firmware updates, uploading, 102
- Front panel
 - CoSign Central Enterprise, 38
 - CoSign Central FIPS HW v7.0, 34
 - DocuSign Signature Appliance Central FIPS HW v8.0, 30
- GetBackup, 152
- GetEvt, 153
- Graphical signature capture device
 - installing, 89
 - model types, 88
- Graphical Signature Management
 - accessing, 90
 - creating an image file, 93
 - creating image-based graphical signature, 92
 - creating text-based graphical signature, 95
 - deleting graphical signature, 92
 - editing graphical signature, 91
 - installing signature capture device, 88
 - overview, 87
 - signature capture mechanisms, 88
 - uploading an image file, 93
 - using application, 89
- Graphical signatures
 - managing, 89
- Group of DocuSign Signature Appliance Users (AD), 116
- Groups command line utility, 155
- Groups management
 - adding a group, 147
 - updating a group, 148
 - viewing groups list, 146
 - viewing groups status, 146
- Hardware
 - installing CoSign Central Enterprise, 37
 - restarting, 108
- Hardware v7.0
 - installing CoSign Central FIPS, 34
- Hardware v8.0
 - installing DocuSign Signature Appliance Central FIPS, 30
- High availability
 - client behavior, 178
 - data replication, 177
 - installation overview, 178
 - installing alternate appliance hardware, 179
 - installing alternate appliance software, 179
 - installing an alternate appliance, 178
 - installing the primary appliance, 178
 - introduction, 177
 - managing data replication, 183
 - managing primary appliance failure, 185
 - overview, 177
 - resubscribing an alternate appliance, 188
 - setting alternate appliance as primary appliance, 185
 - setting primary appliance as alternate appliance, 187
 - Subscribed Alternates window, 183
- Inactivity timeout, clients, 128
- information, viewing in Console for HW before v7.0, 159
- information, viewing in web-based Console, 171
- Install log, downloading, 107
- Installation report, generating, 193
- Installing
 - administrative client, 28
 - administrative client, 27
 - alternate appliance, 178
 - alternate appliance hardware, 179
 - alternate appliance software, 179
 - appliances in a high availability configuration, 178
 - client, centralized installation, 216
 - command line utilities, 151
 - Comodo External CA, 70
 - CoSign appliances HW v7.0, 34
 - CoSign Central Enterprise hardware, 37
 - CoSign Central FIPS hardware v7.0, 34

- DocuSign Signature Appliance as a subordinate CA, 71
- DocuSign Signature Appliance Central FIPS hardware v8.0, 30
- DocuSign Signature Appliance client, 76
- DocuSign Signature Appliance in Active Directory, 40
- DocuSign Signature Appliance in Directory Independent environment, 58
- DocuSign Signature Appliance in LDAP environment, 52
- DocuSign Signature Appliances HW v8.0, 29
 - failed, troubleshooting, 202
 - internal CA, 65
 - overview, 27
 - primary appliance, 178
 - progress bar, troubleshooting, 203, 204
 - ROOT certificate, 96
 - signature capture device, 88
 - troubleshooting, 201
 - uninstalling the administrative client, 29
 - uninstalling the client, 80
 - with reduced privileges, 209
- Installing administrative client
 - installation procedure, 28
 - requirements, 28
- Installing DocuSign Signature Appliance in Active Directory
 - installation procedure, 43
 - overview, 40
 - permissions, 41
 - user types, 51
- Installing DocuSign Signature Appliance in Common Criteria EAL4+ mode
 - installation procedure, 63
- Installing DocuSign Signature Appliance in Directory Independent environment
 - installation procedure, 58
 - overview, 58
- Installing DocuSign Signature Appliance in LDAP environment
 - installation procedure, 53
 - overview, 52
 - supported directories, 52
- Installing with reduced privileges
 - administrating after the installation, 213
 - creating a CDP, 215
 - creating an SCP, 214
 - installation instructions, 212
 - introduction, 209
 - joining to MS domain, 213
 - order of operations, 211
 - overview of regular installation, 210
 - performing user synchronization, 214
 - pre-installation action, 211
 - publishing the ROOT certificate, 214
 - restoring capabilities, 213
 - updating userCertificate, 214
- Intended audience, 13
- Internal CA
 - installing, 65
 - installing DocuSign Signature Appliance as subordinate CA, 71
 - overview, 17
- Introduction
 - to digital signatures, 9
 - to DocuSign Signature Appliance, 9
 - to DocuSign Signature Appliance architecture, 15
- Invalid IP address, 201
- IP address
 - failure when setting via the console interface, 201
 - invalid, 201
 - setting in Console for HW before v7.0, 161
 - setting in Web-based Console, 167
- Key Usage Mask, 123
- Keys
 - central storage of, 16
- Language selection, 79
- Language support, 74
- LDAP
 - Built-in Admin, 119
 - Directory Server Search Base, 118
 - parameters, setting, 127
- LDAP Authentication Method, 127
- LDAP DocuSign Signature Appliance user name, 128
- LDAP DocuSign Signature Appliance user password, 128
- LDAP environment
 - installing DocuSign Signature Appliance software, 52
 - restoring appliance, 139
 - supported directories, 52
- LDAP Secure mode, 127
- LDAP Server Realm name, 127
- LDAP Server UID attribute, 128
- License
 - obtaining new, 114
 - requesting new, 114
 - uploading new, 115
 - viewing expiration date, 161, 173
- Location, 136
- Log files, downloading, 107
- Login for Sign Window, 135
- Logon prompt
 - setting, 124
 - specifying when it appears, 124
 - viewing in SCP, 82
- Mail Server Name, 125
- Mail Server Port, 125
- Managing
 - appliance, 99
 - signatures, 89
- Max Password Failed Attempts, 126
- Maximum Password Validity, 126

- Maximum Repeats in password, 126
- Maximum RSA key pool size, 119
- Maximum Sequence in password, 126
- Microsoft Active Directory
 - adding ROOT certificates to trusted CA list, 97
 - Automatic deployment of client, 216
 - installing DocuSign Signature Appliance software, 40
 - installing with reduced privileges, 209
 - multiple trusted Active Directory, 41
 - parameters, setting, 116
 - permission considerations, 41
 - restoring appliance, 138
 - SCP, 81
 - synchronizing CoSign with, 165
- Minimum Password Length, 126
- Minimum Password Validity, 126
- Modifying system parameters, 116
- Monitoring appliance performance, 113
 - activating monitoring, 113
 - stopping monitoring, 113
 - viewing monitoring results, 114
- Multi-language support, 74
- Multiple trusted Active Directory support, 41
- One Time Password
 - Radius server settings, 133
 - using a Radius Server, 131
- Operating systems supported for client, 75
- OTP devices
 - extended authentication mechanisms, 17
 - management in Radius Server, 20
 - recommendations, 22
- OTP OATH validation window, 134
- OTP validation method, 134
- Outlook, disabling digital signatures, 205
- Overview of DocuSign Signature Appliance, 9
- Packages, defining in SCCM, 217
- Password in Directory Independent environment
 - changing, 86
 - setting policy, 126
- Performance monitoring, 113
- Periodic Directory Sync Timer, 118
- Permissions in Microsoft Active Directory, 41
- Permit upload RSA keys, 119
- PKI
 - DocuSign Signature Appliance's integrated solution, 17
- Primary appliance
 - installing, 178
 - setting as alternate appliance, 187
- Primary DocuSign Signature Appliance
 - overview, 177
- Primary LDAP server address, 127
- Primary LDAP server port, 127
- Prompt for Logon, 124
- Prompt for Signature, 124
- Radius callback list in Common Criteria mode, 134
- Radius customer AD attribute, 134
- Radius Server, 19
 - OTP Management, 20
- Radius Server IP Address, 133
- Radius server parameters, setting, 133
- Radius Server port, 133
- Radius Server Retries, 134
- Radius Server Secret, 134
- Radius Server Timeout, 134
- Refresh timer, certificates, 120
- Refresh window, certificates, 120
- Refreshing certificates, 106
- Regenerate User Key, 119
- Report Apps Names to Event Log, 125
- Report Signatures to Event Log, 125
- Require Static Password Logon, 133
- Resetting tamper mechanism in Console for HW before v7.0, 162
- Resetting tamper mechanism in web-based Console, 170
- Restart server
 - command line utility, 154
- Restarting
 - DocuSign Signature Appliance, 108
 - DocuSign Signature Appliance services, 108
- Restarting appliance in web-based Console, 170
- RestartServer.exe, 154
- RESTful Web Services Support, 129
- Restoring appliance
 - failed appliance restore, troubleshooting, 207
 - in a Directory Independent environment, 139
 - in Active Directory, 138
 - in LDAP environment, 139
 - overview, 138
- Restoring appliance HW v7.0
 - after hard disk failure, 174
- Restoring appliance HW v8.0
 - after hard disk failure, 175
- Restoring factory settings
 - via the Console for HW before v7.0, 163
 - via the web-based Console, 170
- Restoring factory settings for HW v7.0
 - in case of hard disk failure, 174
- Restoring factory settings for HW v8.0
 - in case of hard disk failure, 175
- ROOT certificate
 - adding to trusted CA list, 97
 - downloading, using the Configuration utility, 192
 - installing, 96
 - installing using the Configuration utility, 192
- SAML
 - Accepting Relying Parties Tickets, 136
 - SAML Common Name, 136
 - SAML Display Name, 137
 - SAML Email Address, 136
 - SAML Group Name, 137
 - SAML PN, 136
 - SAML Telephone Number, 136

- SAML Window, 137
- SAML working method, 136
- SAML Common Name, 136
- SAML Display Name, 137
- SAML Email Address, 136
- SAML Group Name, 137
- SAML PN, 136
- SAML Telephone Number, 136
- SAML tickets, 22
 - active mode, 24
 - ADFS, 23
 - passive mode, 23
 - ticket requirements, 24
- SAML Window, 137
- SAML Working Method, 136
- SCCM automatic client deployment
 - advertising a task sequence, 224
 - client installation components, 216
 - creating a task sequence, 217
 - defining and advertising task sequence, 217
 - defining packages, 217
- SCP
 - in a Microsoft Active Directory, 81
 - overview, 81
- Search Base in LDAP Server, 128
- Secondary LDAP server address, 127
- Secondary LDAP server port, 127
- Service Restart operation, 108
- SetSCP, 155
- Setting IP address
 - in Console for HW before v7.0, 161
 - in Web-based Console, 167
- Shutting down
 - CoSign, via the Console for HW before v7.0, 164
 - DocuSign Signature Appliance, 108
 - DocuSign Signature Appliance services, 108
 - DocuSign Signature Appliance, via the web-based Console, 169
- Smart Card Authentication, 131
- SmartCard Authentication Window, 132
- SNMP Accepted Community Name, 135
- SNMP Manager 1, 135
- SNMP Manager 2, 135
- SNMP Monitoring
 - address of the first management system, 135
 - address of the second management system, 135
 - contact name of SNMP agent, 135
 - enabling the SNMP service, 135
 - location name of SNMP agent, 136
 - which members can manage the SNMP agent, 135
- SNMP Service, 135
- Software
 - installation failed, 202
 - installing, 40
 - installing in a Directory Independent environment, 58
 - installing in Active Directory, 40
 - installing in LDAP environment, 52
 - updates, uploading, 102
- SSL certificate, uploading, 112
- SSL proxy
 - specifying IP address, 129
 - specifying password, 129
 - specifying port number, 129
 - specifying usage, 128
 - specifying user name, 129
- SSL Proxy IP, 129
- SSL Proxy Password, 129
- SSL Proxy Port, 129
- SSL proxy settings, 68
- SSL Proxy User Name, 129
- Starting the Administration MMC, 99
- Static IP address, using in Console for HW before v7.0, 161
- Storage of keys in DocuSign Signature Appliance, 16
- Subordinate CA
 - installation, 71
 - introduction, 67
 - renewing certificate, 110
- Support
 - DocuSign support contact information, 201
- Switch to prime appliance
 - command line utility, 154
- Switch2Prim.exe, 154
- Synchronization timer, directory, 117
- Synchronizing DocuSign Signature Appliance with external CA in automated mode, 105
- Synchronizing DocuSign Signature Appliance with the directory service, 104
- Syslog Server IP Address, 126
- System
 - does not respond, troubleshooting, 206
- System parameters
 - Accepting Relying Parties Tickets, 136
 - Add Certificate to CRL, 122
 - Additional Radius IPs (CC Mode), 134
 - AIA Publication Location, 121
 - Allow Get Backup Anonymously, 130
 - Alternate Extended Auth Mode, 132
 - Alternate Radius Server IP Address, 133
 - Alternate Radius Server Port, 134
 - Appliance Administrator Group, 117
 - Automatic Deletion of Users, 117
 - Biometric Authentication, 131
 - Biometric Authentication Window, 132
 - Biometric Shared Secret, 132
 - Built-in Admin, 119
 - CA Cert Hash Algorithm, 122
 - Case Sensitive Username, 130
 - Certificate Common Name, 121
 - Certificate Expiration Variance, 120
 - Certificate Issuer Name, 133
 - Certificate Refresh Timer, 120
 - Certificate Refresh Window, 120

- Certificate Validity Period, 122
- Clients Inactivity Timeout, 128
- Cloud Monitoring, 131
- Cloud Site ID, 131
- Common Criteria Mode, 130
- Common Criteria Type, 130
- Contact Name, 135
- CORS domain for REST API, 130
- CPS Object ID, 122
- CPS URI, 122
- Create Computer Keys, 118
- Create Group Keys, 118
- Create User Key Mode, 119
- CRL Publication Location, 121
- CRL Publishing Frequency, 120
- CRL Retrieval, 133
- CRL Validity Period, 121
- Debug Level, 128
- Default Radius password length, 133
- Delete expired users by window, 123
- Directory Server Search Base, 118
- Directory Synchronization Timer, 117
- Email From Address, 126
- Enable Automatic User Logon, 124
- Enable the Radius AD attribute, 134
- Enable User Counters, 125
- Enforce CRL Validation, 133
- Enforce FIPS Approved Algorithms, 130
- Enhanced Key Usage Enabled, 123
- Enhanced Key usage Mask, 123
- Event log storage period, 125
- Expired user action, 122
- Extended Authentication Method, 131
- External CA Password, 123
- External CA User Name, 123
- Extractable Keys, 119
- Group of DocuSign Signature Appliance Users (AD), 116
- Key usage Mask, 123
- LDAP Authentication Method, 127
- LDAP DocuSign Signature Appliance user name, 128
- LDAP DocuSign Signature Appliance user password, 128
- LDAP Secure mode, 127
- LDAP Server Realm name, 127
- LDAP Server UID attribute, 128
- Location, 136
- Login for Sign Window, 135
- Mail Server Name, 125
- Mail Server Port, 125
- Max password failed attempts, 126
- Maximum Password Validity, 126
- Maximum Repeats in password, 126
- Maximum RSA key pool size, 119
- Maximum Sequence in password, 126
- Minimum Password Length, 126
- Minimum Password Validity, 126
- missing from Administration MMC, 205
- modifying, 116
- One Time Password using a Radius Server, 131
- OTP OATH validation window, 134
- OTP validation method, 134
- Periodic Directory Sync Timer, 118
- Permit upload RSA keys, 119
- Primary LDAP server address, 127
- Primary LDAP server port, 127
- Prompt for Logon, 124
- Prompt for Signature, 124
- Radius customer AD attribute, 134
- Radius Server IP Address, 133
- Radius Server Port, 133
- Radius Server Retries, 134
- Radius Server Secret, 134
- Radius Server Timeout, 134
- Regenerate User Key, 119
- Report Apps Names to Event Log, 125
- Report Signatures to Event Log, 125
- Require Static Password, 133
- RESTfulWeb Services Support, 129
- SAML Common Name, 136
- SAML Display Name, 137
- SAML Email Address, 136
- SAML Group Name, 137
- SAML Telephone Number, 136
- SAML UPN, 136
- SAML Window, 137
- SAML Working Method, 136
- Search Base in LDAP Server, 128
- Secondary LDAP server address, 127
- Secondary LDAP server port, 127
- Smart Card Authentication, 131
- SmartCard Authentication Window, 132
- SNMP Accepted Community Name, 135
- SNMP Manager 1, 135
- SNMP Manager 2, 135
- SNMP Service, 135
- SSL Proxy IP, 129
- SSL Proxy Password, 129
- SSL Proxy Port, 129
- SSL Proxy User Name, 129
- Syslog Server IP Address, 126
- Use AIA Location Settings, 121
- Use CDP Location Settings, 121
- Use SmartCard Auth for Logon, 132
- Use SSL Proxy, 128
- User Activation, 125
- User Certificate Publishing, 118
- User Must Change Password, 126
- Users Administrator Group, 117
- Users Key Length, 119
- Web Services Support, 129
- Tamper evidence, 21
- Tamper mechanism

- resetting in Console for HW before v7.0, 162
- resetting in web-based Console, 170
- Tamper response, 21
- Task sequence
 - advertising in SCCM, 224
 - creating in SCCM, 217
- Terminal server, deploying client on, 76
- Terminal, configuring for console, 157
- time and date, setting in , web-based Console, 167
- Time, setting in , web-based Console, 167
- Time, setting in Console for HW before v7.0, 164
- Touch screen of web-based Console, 174
- Troubleshooting
 - Administration MMC operation fails, 206
 - administrative problems, 205
 - alternate installation, 203
 - appliance does not start, 204
 - appliance not in factory settings mode, 202
 - backup fails, 207
 - cannot see personal certificates, 205
 - client-related problems, 204
 - console-related problems, 204
 - default values do not appear in the directory setup dialog box, 202
 - installation, 201
 - installation fails, 202
 - installation issues, 203
 - IP address invalid, 201
 - overview, 201
 - parameters missing from Administration MMC, 205
 - progress bar during installation, 203
 - restore operation fails, 207
 - setting IP address via the console, 201
 - signatures in Outlook, 205
 - system does not respond, 206
 - users do not receive certificates, 206
- Trusted CA list, adding ROOT certificates to, 97
- Turnkey solution, 17
- Uninstalling
 - administrative client, 29
 - DocuSign Signature Appliance client, 80
 - DocuSign Signature Appliance client using DocuSign Signature Appliance CD, 80
- Updates, uploading, 102
- Upgrading
 - overview, 102
 - to version 7.1, 102
 - to version 7.4, 103
 - to version 7.5, 103
 - to version 8.0, 103
- Uploading updates, 102
- USB to serial adaptor, 158
- Use AIA Location Settings, 121
- Use CDP Location Settings, 121
- Use SmartCard Auth for Logon, 132
- Use SSL Proxy, 128
- User
 - authentication, 16
 - enrollment, 15
- User Activation, 21, 125
- User Activation, 86
- User Certificate Publishing, 118
- User groups, 116
- User Must Change Password, 126
- Users Administrator Group, 117
- Users do not receive certificates, troubleshooting, 206
- Users Key Length, 119
- Users Management utility
 - activating, 141
 - adding a user, 144
 - deleting a user, 145
 - displaying user information, 146
 - generating a Users report, 143
 - login, 143
 - login using built-in administrator, 144
 - logout, 144
 - main window, 142
 - managing groups, 146
 - menus, 143
 - overview, 140
 - resetting a user's password counter, 144
 - resetting a user's signature counters, 144
 - resetting signature counters, 143
 - right-click menu, 150
 - setting user password, 146
 - status bar, 143
 - toolbar, 150
 - user fields, 142
- Validating signatures
 - installing CoSign verifier, 96
 - installing ROOT certificate, 96
 - using CoSign verifier, 97
- Viewing
 - certificates in store, troubleshooting, 205
 - CoSign information in console for HW before v7.0, 159
 - information in web-based Console, 171
- Web server, deploying client on, 76
- Web Services Support, 129

