

DocuSign Signature Appliance Administrator Guide

Version 9.3

Copyright ©2003-2019 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) 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
December 2019

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 11
Requirements for Data Authentication Systems 11
Introduction to DocuSign Signature Appliance (DocuSign SA) 11
Environments Supported by DocuSign SA 12
Applications that Work with DocuSign SA 12
DocuSign SA Components 12
DocuSign SA Guides 13
DocuSign Signature Appliance Hardware Models 14
End User Platforms 14
Installing the Appliance in Hardware Security Model (HSM) Mode 15
Intended Audience 15
Chapter 2: DocuSign SA Architecture and Data Flow 16
Enrollment Using a Standard User Management Application 16
Central Storage of Signing Keys 17
User Authentication 17
Extending User Authentication 17
Turnkey Solution 18
Directory Independent Environment 18
Using DocuSign SA's Internal CA 18
Using DocuSign SA in Manual External CA Mode 19
Using DocuSign SA in Automatic External CA Mode 19
Multiple CA support 20
Using DocuSign SA in Common Criteria EAL4+ Deployments 20
Extended Authentication using an internal OTP mechanism 21
Extended Authentication using an External Radius Server 21
User Activation 22
Signature key Generation and Certificate Enrollment 23
Physical Security: Tamper Evidence and Tamper Response 23
Recommended OTP Devices 24
Using SAML/JWT Tickets to Authenticate DocuSign SA Users 24

ADFS Typical Workflow 25
Passive Mode using the DocuSign SA Web App and DocuSign SA Connector for SharePoint 25
Active Mode Using the DocuSign SA Client 26
SAML Ticket Requirements 26
Chapter 3: Installing DocuSign SA 28
Installing the DocuSign SA Administrative Client 28
Installation Requirements 29
Installing the DocuSign SA Administrative Client 30
Uninstalling the DocuSign SA Administrative Client 32
Installing the DocuSign Signature Appliance Hardware version 8.0 33
Installing the DocuSign SA FIPS Appliance Hardware 8.0 33
Installing the DocuSign SA Enterprise Hardware 8.1 38
Installing the DocuSign Signature Appliance Software 40
Installing DocuSign SA in a Microsoft Active Directory Environment 41
Installing DocuSign SA in an LDAP based Environment 52
Installing DocuSign SA in a Directory Independent Environment 60
Installing DocuSign SA in a Common Criteria EAL4+ Mode as a Signature Creation Device or Seal Creation Device 65
Installing an Internal Certificate Authority 69
Using an External CA in Manual Mode 73
Using an External CA in Automated Mode 73
Creating a Symantec Profile Preparatory to Configuring Symantec as DocuSign SA's External CA 86
Installing DocuSign SA as a Subordinate CA 99
Multi-Language Support 102
Chapter 4: Deploying the DocuSign SA Client 103
Deploying the Client 103
Deployment Options 103
Installing the DocuSign SA Client 104
Uninstalling the DocuSign SA Client 108
Distributing DocuSign SA Information through the SCP 109
Using the DocuSign SA Client System Tray Icon Options 111
Administrator Actions 111

Installing the Root Certificate....112
Adding the ROOT Certificate to a Trusted CA List (Active Directory only) 112
Extended Authentication Mode....113
Chapter 5: Managing the DocuSign Signature Appliance....114
Prerequisites to Using the DocuSign SA Administration MMC....114
Starting the DocuSign SA Administration MMC....114
DocuSign SA Administration MMC Capabilities....116
Backing up the DocuSign SA Data....116
Shutting Down and Restarting DocuSign SA Services....117
Restarting the DocuSign Signature Appliance....117
Upgrading DocuSign SA....118
Upgrading to Version 8.5....118
Upgrading to Version 8.51 (system upgrade)....118
Upgrading to Version 9.0....119
Upgrading to Version 9.1....119
Upgrading to Version 9.3....119
Uploading a Software Update....119
Additional Security related updates....120
Uploading Certificate material to DocuSign SA....120
Upload certificates....121
Uploading an SSL Certificate....121
High Availability....122
Downloading Log Files....123
Renewing the DocuSign CA's RA certificate....128
Renewing the Symantec Authentication Key File....130
Monitoring Performance Parameters of the DocuSign Signature Appliance....131
Activating Performance Monitoring....131
Stopping Performance Monitoring....131
Viewing Performance Parameters....132
Monitoring Network Packets to/from the DocuSign Signature Appliance....132
Activating Network Capturing....132
Stopping Network Capturing....133
Downloading captured networking packets....133

Obtaining a New DocuSign SA License....133
Requesting a New License....133
Uploading the New License....134
Advanced Options for Active Directory or LDAP Deployments....135
Resyncing the Appliance Clock with Active Directory....135
Changing a regular Active Directory deployment to Multiple Domain deployment....135
Re-Joining an Appliance to the AD Domain....136
Synchronizing DocuSign SA with the Directory Service....136
Managing Certificate Authorities in the DocuSign Signature Appliance....138
Adding a new CA....138
Managing the list of CAs....140
Synchronizing DocuSign SA with the External CA in Automated mode....140
Refreshing Certificates....141
Renewing the Subordinate CA Certificate....141
Disabling a CA....143
Setting CA parameters....143
Changing DocuSign SA System Parameters....147
Users Directory Parameters....148
Key Management Parameters....150
Certificate Management Parameters....152
Client Security Setting Parameters....152
Auditing and Accounting Parameters....154
Alerts and Notifications Parameters....155
Password Policy....155
LDAP....156
Advanced Parameters....157
Extended Authentication....161
SNMP....163
SAML....164
JWT....166
Internal OATH TOTP....167
Restoring the DocuSign Signature Appliance....167
Restoring the DocuSign Signature Appliance in Microsoft Active Directory....168

Restoring the DocuSign Signature Appliance in an LDAP Environment....169
Restoring the DocuSign Signature Appliance in a Directory Independent Environment..169
Using the Users Management Utility....170
Activating the Users Management Utility....171
Users Management Main Window....172
Users Management Window Status Bar....173
Users Management Menus....173
Users Management Toolbar....183
Using Command Line Utilities....186
GetBackup....186
GetEvt....187
restartServer.exe....188
Switch2Prim.exe....189
SetSCP....190
getServerReport....190
AuditLogDownloadUtility.exe....191
Chapter 6: Using the DocuSign SA Console....194
Accessing the DocuSign SA Console....194
Using the DocuSign SA Web-based Console....194
Setting the Appliance IP Address....196
Setting Time....197
Shutting Down....199
Restarting the Appliance....199
Resetting the Tamper Mechanism....199
Restoring Factory Settings....200
Copying the Backup Minikey....201
Checking whether Security Information in the Appliance Matches Security Information in the Minikey Token....205
Upload Software....206
Download Server Logs....207
Displaying DocuSign Signature Appliance Status....208
Using the Touch Screen of a DocuSign SA v8.0 Appliance....212
Restoring the DocuSign Signature Appliance after an Internal Hard Disk Failure....212

In Appliance Hardware v8.1 Enterprise model 212
In DocuSign SA Hardware V8.0 – Appliance FIPS model 213
Chapter 7: Configuring High Availability 215
Overview of High Availability 215
Installing DocuSign Signature Appliances in a High Availability Configuration 217
Installing the Primary DocuSign Signature Appliance 217
Setting the Communication Protocol between the Primary Appliances and Alternate Appliances 217
Installing an Alternate DocuSign Signature Appliance 218
Managing the Alternate DocuSign Signature Appliance 222
Managing Data Replication in the Alternate DocuSign Signature Appliance 223
Viewing Replication Status of an Alternate DocuSign Signature Appliance 223
Re-initializing an Alternate DocuSign Signature Appliance 224
Unsubscribing an Alternate DocuSign Signature Appliance 224
Managing Primary Appliance Failure and Recovery 224
Setting an Alternate Appliance to be the Primary Appliance 224
Setting a Previous Primary Appliance to be an Alternate Appliance 227
Re-subscribing an Alternate Appliance with a Primary Appliance 228
Upgrading Appliances Participating in a High Availability Cluster 228
Chapter 8: DocuSign SA Configuration Utility 230
Overview 230
Using the DocuSign SA Configuration Utility 230
DocuSign SA Configuration Utility Menus 232
Running the DocuSign SA Configuration Utility in Admin Mode 234
Configuration File Operations 236
Group Policies Operations 237
Running the DocuSign SA Configuration Utility in End User Mode 238
Distributing the DocuSign SA Client Configuration 238
Distributing the DocuSign SA Configuration Using Configuration Files 238
Distributing the DocuSign SA Configuration Using Group Policy 239
Setting Admin Configuration 240
Admin – Appliance Installation 240
Admin – Performance Monitoring 242

Chapter 9: Troubleshooting 243
Installation Problems 243
DocuSign SA IP Address is Invalid 243
Error When Setting the DocuSign SA IP Address Via the Console Interface 243
Default Values Do Not Appear in the Directory Setup Dialog Box 244
The Appliance is Not in Factory Settings Mode 244
Installation Failed 244
Error During Installation 245
Progress Bar Stops Advancing 245
DocuSign Signature Appliance Installation Issues 245
Error when communicating with DocuSign CA or DocuSign TSCP CA 245
High Availability/Load Balancing – Alternate Installation 246
DocuSign Signature Appliance Problems 246
DocuSign Signature Appliance Does Not Start 246
Console Problems 246
Client-Related Problems 247
Cannot Enable the “Add Digital Signature to Outgoing Messages” Checkbox in Outlook 247
Cannot See Any Certificates in Store 247
Administrative Problems 248
DocuSign SA System Parameters Do Not Appear in the DocuSign SA Administration MMC 248
All DocuSign SA Administration MMC Operations Fail 248
DocuSign SA Does Not Respond 248
New Users Do Not Receive Certificates 249
Restore Appliance Fails 249
Backup DocuSign SA Operation Fails 250
Appendix A: DocuSign SA Installation with Reduced Privileges 251
Overview 251
Regular DocuSign SA Installation 252
Creating a New Computer Account for the DocuSign Signature Appliance 252
Joining the DocuSign Signature Appliance to MS Domain 252
Creating a Services Connection Point (SCP) 252

DocuSign SA User Synchronization 252
Updating the userCertificate Attribute for Users 252
DocuSign SA CA Root Certificate Information 253
DocuSign SA CA CDP (Certificate Distribution Point) 253
DocuSign SA Installation with Reduced Privileges 253
Preliminary Action – Adding the DocuSign SA Computer to the Domain 253
Installing DocuSign SA in a Reduced Privileges Environment 254
Complementing the DocuSign SA Installation with Missing Capabilities 255
Appendix B: Centralized DocuSign SA Client Installation 258
Automatic Client Deployment using Microsoft SCCM 258
DocuSign SA Installation Components 258
Defining and Advertising a DocuSign SA Client Task Sequence 259
Step 1: Define DocuSign SA Packages 259
Step 2: Create a Task Sequence 260
Step 3: Advertise the Task Sequence 264
Appendix C: Requirements for Accessing External Resources 266
Automated External CA – DocuSign CA or DocuSign TSCP CA 266
Automated External CA – Comodo 266
Automated External CA – Symantec 266
General CRL/AIA/OCSP access for a Certificate Authority 267
DSA is deployed in an LDAP environment with SSL/TLS 267
Certificate of IDP (Identity Provider) that produces the SAML Tokens 267
Certificate validation performed as part of the DocuSign SA REST/SOAP 267
Appendix D: WinPcap Copyright Notice 268
Index 273

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 SA)

DocuSign SA is a PKI-based, off-the-shelf digital-signature solution that can be integrated with a wide range of applications. In this way, DocuSign SA enables organizations to embed digital signatures in various documents, forms, and transactions. DocuSign SA 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 SA 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 SA

DocuSign SA 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 SA was installed.

DocuSign SA 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 SA

An increasing number of applications can work with DocuSign SA as their digital-signature layer, including:

- Microsoft Office 2010/2013/2016 (Word, Excel, and PowerPoint)
- Microsoft InfoPath 2010/2013
- Adobe Acrobat/Reader
- Foxit Reader
- Microsoft SharePoint 2010/2013/2016/2019
- XML
- Microsoft Outlook and Outlook Express
- Adobe Server forms (for signing web forms)
- AutoCAD
- OpenText
- Web applications
- Any application that has a *print* option can use DocuSign SA to generate a PDF file and sign it.

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

DocuSign SA Components

DocuSign SA 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 SA*.
  The DocuSign Signature Appliance can be interfaced either through installed DocuSign SA client software or through a Web Services interface that can be based on either a SOAP or RESTful API.
- **Client** – The DocuSign SA Client software, installed on the users' computers. For more information, refer to *Chapter 4: Deploying the DocuSign SA Client*.
- **Administrator** – The DocuSign SA Administrative software that includes the DocuSign SA Microsoft Management Console (MMC) snap-in, installed on the administrative computer. For more information, refer to *Chapter 5: Managing the DocuSign Signature Appliance*.
- **DocuSign SA 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.
- **DocuSign SA 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. DocuSign SA Web App can use the local DocuSign Signature Appliance for performing digital signature operations.
  Applications can interact with the DocuSign SA Web App and add a digital signature to documents using a web based interface.
- **DocuSign SA 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 SA Appliance via a DocuSign SA RESTful interface.
  The DocuSign SA Mobile App can interface with either the organizational DocuSign SA Appliance, or DocuSign SA's Trial system.
- **DocuSign SA Signature APIs** – Developers can use local and network APIs to integrate their applications with DocuSign SA appliances.

DocuSign SA Guides

DocuSign SA 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 in which DocuSign SA can operate.
- *DocuSign Signature Appliance User Guide* – Provides all the information necessary for an end user to use DocuSign SA. Includes information about special add-ins for various applications such as Microsoft Office.
- *DocuSign Signature Appliance Connector for SharePoint User Guide* – Provides all the information necessary for implementing and using the DocuSign SA Connector for SharePoint.
- *DocuSign Signature Appliance Web App User Guide* – Provides all the information necessary for deploying DocuSign SA Web App in the organization's environment.

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

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 SA Enterprise Model* – The hardware is based on a rack-mountable 1U box packaged in a standard commercial casing.
- *DocuSign SA FIPS Model* – 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 SA in Common Criteria EAL4+ deployments.

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

End User Platforms

DocuSign SA 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 DocuSign SA Client. For example, end users can sign using DocuSign SA Prepare & Sign, 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. DocuSign SA offers:
  - Microsoft SharePoint integrated with DocuSign SA Connector for SharePoint, enabling the end user to sign documents or data stored inside SharePoint.
  - The DocuSign SA 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 DocuSign SA Mobile App enables end users to sign documents using their mobile devices. The Mobile App can be installed either on Android devices or iOS devices.
  The DocuSign SA 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.

Installing the Appliance in Hardware Security Model (HSM) Mode

Starting from DSA version 9.0, you can install the Appliance in HSM mode. The HSM mode of the Appliance serves other use cases such as symmetric encryption and managing a Certificate Authority signature key.

Accessing the Appliance in HSM mode is possible through a special client software called DocuSign HSM client. For more information, refer to the DocuSign HSM manuals.

Intended Audience

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

Chapter 2: DocuSign SA Architecture and Data Flow

DocuSign SA is a hardware appliance that is installed on the network. The appliance includes all the necessary components for PKI-based digital signatures. DocuSign SA 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 SA signs all of the user's signing requests using the user's signing credentials.

Figure 1 illustrates the DocuSign SA architecture.

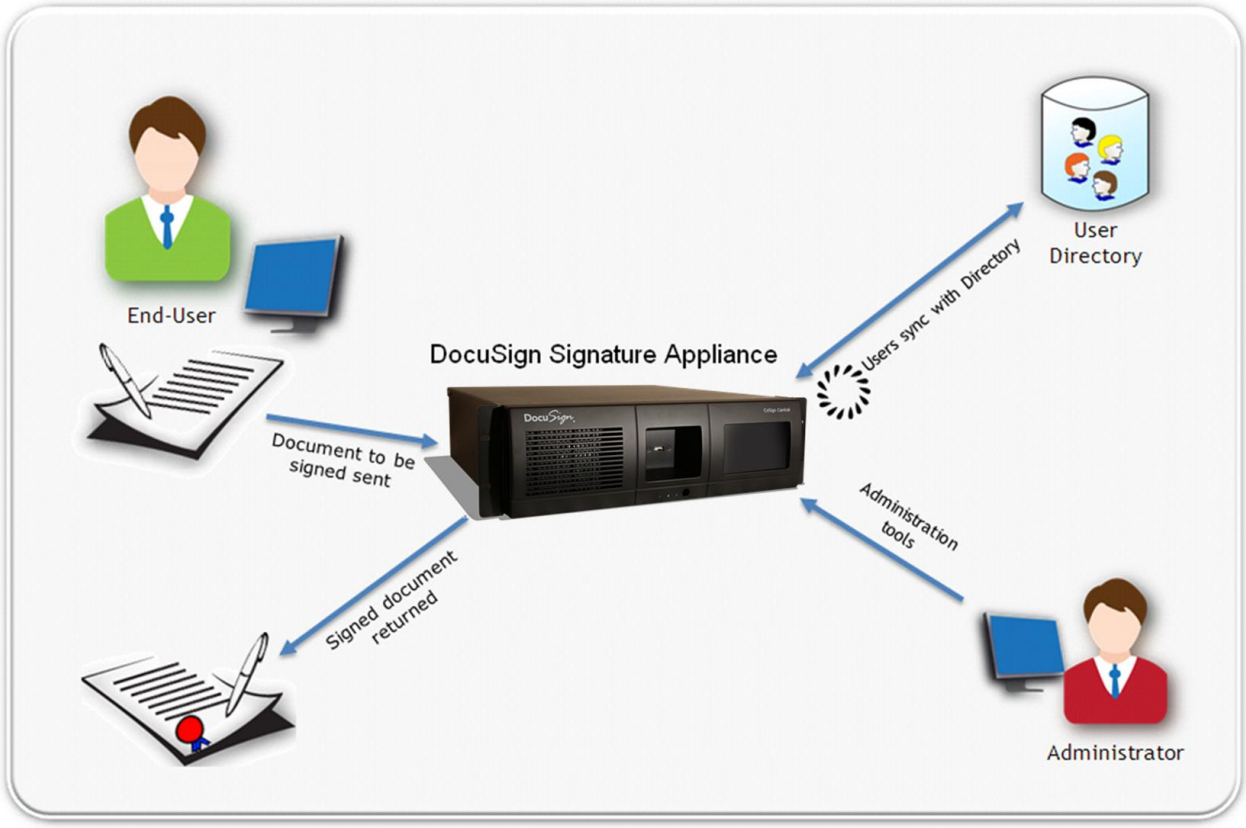


Figure 1 DocuSign SA Architecture

Enrollment Using a Standard User Management Application

With DocuSign SA, 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 SA 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 SA, 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 SA'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 SA 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 SA with the user's credentials (in the case of Microsoft Active Directory, credentials are sent automatically).
3. DocuSign SA finds the correct signing key for the user and signs the document with this key.
4. DocuSign SA returns the signature to the requesting application.

Extending User Authentication

You can configure DocuSign SA 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 SA allows accessing the user's key and performing the digital signature operation.

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

- *One Time Password (OTP)* – The user uses an OTP mechanism such as Google Authenticator. 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 SA 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.

Turnkey Solution

DocuSign SA provides a complete and integrated digital-signature system. DocuSign SA integrates the different components required by a digital-signature system along with a graphical signature capture mechanism. Since DocuSign SA 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 SA 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 SA can also be used by organizations that maintain their own proprietary user-management system.
When DocuSign SA is installed in a Directory Independent environment, the organization's administrator can either use DocuSign SA's users management utility or an application developed by the organization to create DocuSign SA users and consequently generate keys and certificates for the new DocuSign SA users.

These DocuSign SA users are just like DocuSign SA 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 SA (currently, Microsoft Active Directory or LDAP-based directory). DocuSign SA enables these organizations to manage the DocuSign SA users through GUI-based user management utilities.

Using DocuSign SA's Internal CA

DocuSign SA 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 SA 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 SA's internal CA certificate certified by the organization's CA, thus DocuSign SA acts as a subordinate CA.

Using DocuSign SA in Manual External CA Mode

DocuSign SA 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 SA, and is not part of the DocuSign SA solution.

When DocuSign SA is installed in manual external CA mode, DocuSign SA 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 DocuSign SA 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 DocuSign SA CA.
- Cases where the certificate must be provided by an external CA that is not currently supported by DocuSign SA's 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 SA 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 DocuSign certificate authority or Symantec certificate authority can 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.

The DocuSign certificate authority interface is available from DocuSign Signature Appliance version 9.3. There are two flavours of using the DocuSign certificate Authority:

- DocuSign TSCP CA – Can be used only with the DocuSign FIPS model
- Regular DocuSign CA – Can be used with both the FIPS and the Enterprise hardware model

The Symantec certificate authority interface is available in DocuSign Signature Appliance version 8.1 and starting from DocuSign Signature Appliance version 8.4.
Appliance version 8.1 can be used only with DocuSign SA FIPS hardware version 8.0.

Communication with the external CA is based on the TLS Protocol, where TLS1.0, TLS1.1 and TLS 1.2 are supported.

From DocuSign Signature Appliance version 9.3, Comodo external CA is not supported any more.

Multiple CA support

Starting from DocuSign SA version 8.5, it is possible to define and associate multiple Certificate Authorities with a specific DocuSign Signature Appliance, and assign users to different CAs according to the organization's requirements. This may also be used in cases where DocuSign SA is deployed in a service that supports different organizations or different organizational units.

In a multiple CA deployment, the CA created during Appliance installation is the default CA. Only the default CA can be configured to interact with external CAs in automated mode. The additional CAs must be based on an Internal CA deployment.

Each user is assigned a CA based on his/her group membership. If a user is not a member of a group, the user is assigned the default CA.

Using DocuSign SA in Common Criteria EAL4+ Deployments

The DocuSign SA 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 SA is installed in Directory Independent mode. This means that the DocuSign Signature Appliance is not synchronized with any external users directory.

DocuSign SA can be installed 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 internal OTP mechanism

Starting from DocuSign Signature Appliance version 9.0, you can configure the Appliance to use an internal time-based OTP mechanism.
The OTP generator shared secret is generated for every user, and the secret can be downloaded once to an OTP generation device (for example, a Google Authenticator App deployed on the end user's mobile phone).
As part of the process of creating a digital signature, the user is requested to enter an OTP. The OTP is presented in the user's OTP device (for example, the user's mobile phone).

Only after a proper validation of the OTP by the DocuSign Signature Appliance, does the Appliance proceed to perform the digital signature operation.

You can use this mechanism also in Common Criteria EAL4+ deployment when DocuSign SA is deployed as a Signature Creation Device.

Extended Authentication using an External Radius Server

In a Common Criteria EAL4+ deployment when DocuSign SA 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 SA 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 DocuSign.

The Radius Server should be installed and configured so that DocuSign SA will interface the Radius Server using a Radius Protocol, and the Radius Server will access the DocuSign Signature Appliance using the DocuSign SA 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 SA 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 SA 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 SA is installed as a Seal Creation Device.

The new user uses the DocuSign SA 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 SA 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 SA 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 SA client is installed.
These tools can use either the DocuSign SA API (DocuSign SA Signature Local API or DocuSign SA 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 SA API (DocuSign SA Signature Local API or DocuSign SA Signature API) or other APIs (such as PKCS#11, Microsoft CAPI or JAVA JCA interface), which are offered by the DocuSign SA Client software.

Physical Security: Tamper Evidence and Tamper Response

The DocuSign SA FIPS hardware model 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 SA 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 SA*).

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/JWT Tickets to Authenticate DocuSign SA Users

You can log into DocuSign SA using a SAML ticket or a JWT (Jason Web Token) ticket.

When a user presents a SAML/JWT 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/JWT ticket.

One of the benefits of accepting SAML/JWT tickets for authenticating users is to make DocuSign SA services available to new user communities. For example, suppose Company A would like to enable users from company B to connect to DocuSign SA 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 Typical* Workflow and to Microsoft documentation, such as: http://msdn.microsoft.com/en-us/library/bb897402.aspx.

Starting from DocuSign SA version 8.4, SAML/JWT can be used also when the DocuSign Signature Appliance is deployed in Active Directory mode or LDAP mode. In these cases, users can communicate with the DocuSign Signature Appliance using either their regular credentials or SAML/JWT tickets. However, make sure that the identity of the user in Active Directory and in the SAML/JWT system are aligned. Failures may occur (especially when connecting to Alternate

Appliances) when connecting with a JWT/SAML ticket that includes an identity that does not exist in Active Directory.

> ***Note:*** SAML/JWT tickets cannot be used if DocuSign SA is deployed in a Common Criteria EAL4+ mode.

ADFS Typical Workflow

The ADFS/SAML typical 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 SA 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 SA and should be loaded to DocuSign SA by right-clicking the relevant DocuSign Signature Appliance and selecting **All Tasks → Upload Certificates → Upoad ROOT Certificate Chain** in the DocuSign SA Signature Appliance Management Console.

Passive Mode using the DocuSign SA Web App and DocuSign SA Connector for SharePoint

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

1. The end user connects to his organizational URL in the DocuSign SA Web App that is dedicated to that user's organization.
2. The DocuSign SA 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/JWT ticket.

3. The user is redirected back to the DocuSign SA Web App with the provided SAML/JWT ticket.
4. The DocuSign SA Web App accesses the DocuSign Signature Appliance with the supplied SAML/JWT 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/JWT ticket. It is assumed that the email address is unique.
5. The user continues with his/her web session.

Note: If the DocuSign SA 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 DocuSign SA 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 SA 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 SA client and configure the DocuSign SA client to use SAML/JWT based authentication. For more information, refer to the *DocuSign SA User Guide*.

SAML Ticket Requirements

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

- The SAML ticket must be version 1.1, version 2.0, or SAML Protocol version 2.0.
- Date/Time restriction – Every SAML/JWT ticket is valid for a given period. Make sure to provide SAML/JWT tickets that are still valid.
- The SAML/JWT 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 DocuSign SA *SAML Working Method* system parameter has a value of 2.
  - ***Audience –*** This mandatory field should contain a URL that defines the DocuSign SA Service. This URL should be identical to the URL defined in the DocuSign SA *Accept 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 or SAML2-Protocol based server. The local ADFS server or SAML2-Procotol

based 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/JWT ticket parameters names (such as **upn** or **emailaddress**) can be modified in the *SAML* and *JWT* sections of the DocuSign SA system parameters.

Chapter 3: Installing DocuSign SA

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

DocuSign SA installation consists of several steps:

1. Installing the DocuSign SA administrative client. The DocuSign SA administrative client includes various administrative utilities, as well as the Microsoft Management Console (MMC), DocuSign SA's administration snap-in. The DocuSign SA administrative client installation is described in this chapter.
2. Installing the DocuSign SA Enterprise / DocuSign SA 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 SA in Common Criteria EAL4+ mode). Appliance software installation is described in this chapter.
4. Deploying the DocuSign SA Client, in a Microsoft-Active Directory environment, LDAP based directory, or Directory Independent environment. This is described in *Chapter 4: Deploying the DocuSign SA Client*.
5. Using the DocuSign SA console. This is described in *Chapter 6: Using the DocuSign SA Console*.
6. Using the graphical signature management application that enables setting a graphical signature for users of the organization. This is described in the *DocuSign SA User Guide*.
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: DocuSign SA installation differs slightly depending on whether DocuSign SA is being installed in a Microsoft Active Directory environment, LDAP based environment, or Directory Independent environment. These differences are mentioned where applicable.

Installing the DocuSign SA Administrative Client

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

- Administrate DocuSign Signature Appliances, using the DocuSign SA Administration MMC. For more information, refer to *Chapter 5: Managing the DocuSign Signature Appliance*.
- Administrate DocuSign SA users. For more information, refer to *Using the Users Management Utility*.
- Set end users configuration. For more information, refer to *Chapter 8: DocuSign SA Configuration Utility*.

Installation Requirements

The DocuSign SA 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.
- Windows 2016 Server.

When installing the DocuSign SA 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 DocuSign SA administrative client must have domain administrative rights.

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

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

Installing the DocuSign SA Administrative Client

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

To install the DocuSign SA administrative client:

1. Activate the *DSA Setup64.exe* installation program.
2. The Choose Setup Language window appears.

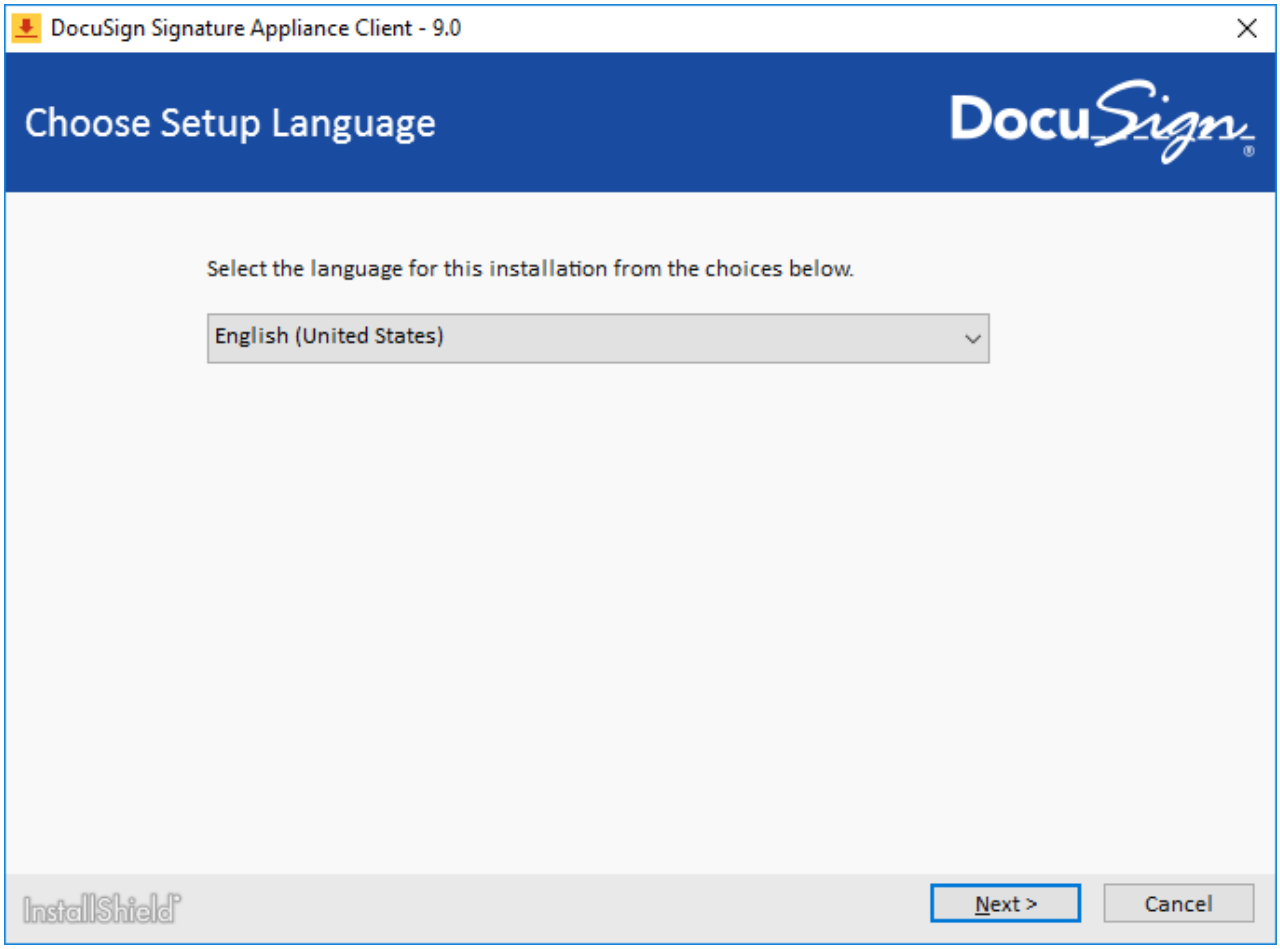


Figure 2 Choose Setup Language Screen

3. Choose your preferred language from the list. Click **Next.** The following screen appears.

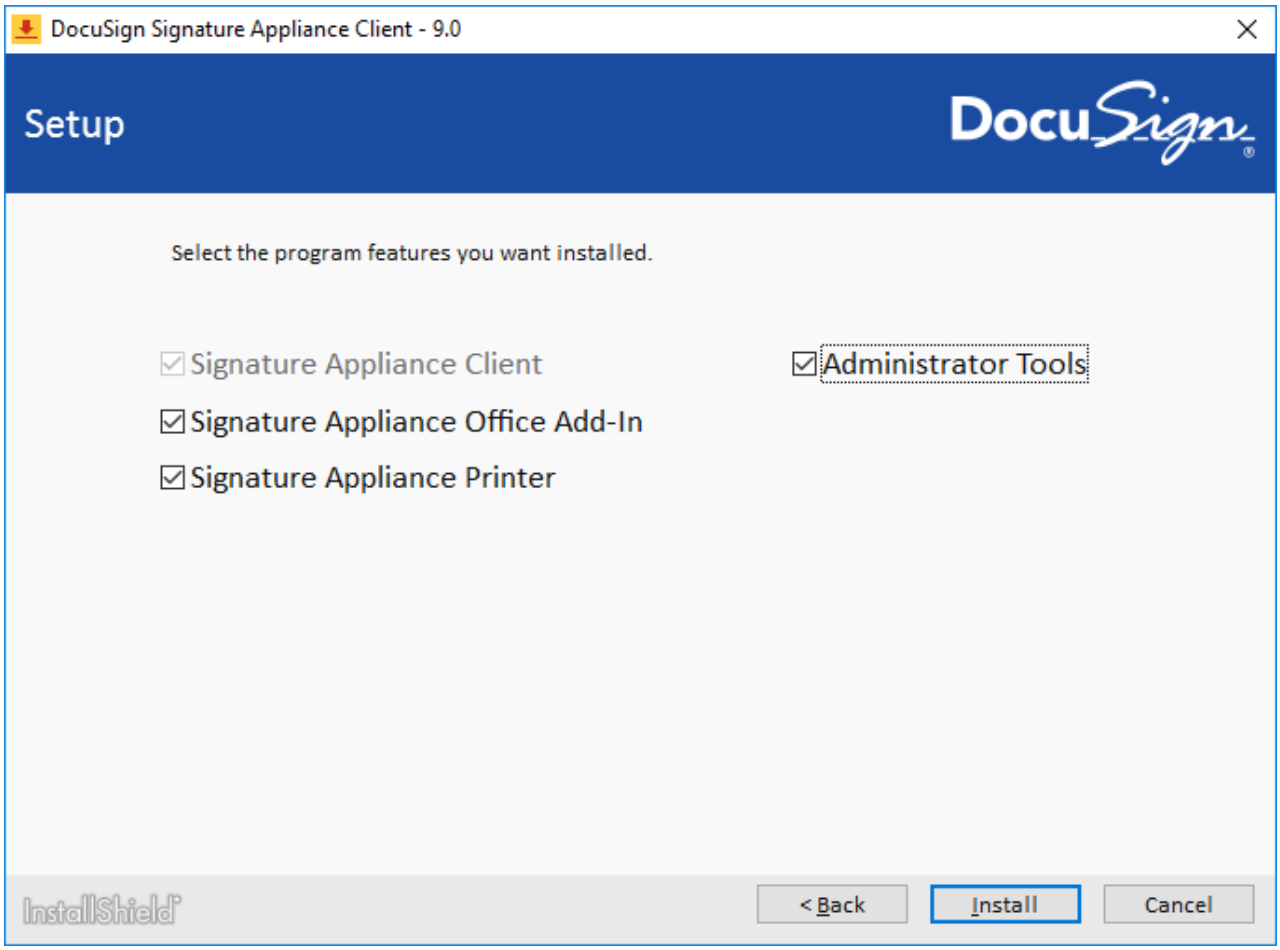


Figure 3 Select the Program Features You Want Installed

4. Select the following components:
   - **Signature Appliance Client** (this option is pre-selected)**.**
   - **Administrator Tools**

   Note: you can select other components as well, depending on the intended usage of the installed desktop.

5. Click **Install.** A progress bar appears, indicating the installation status of the various DocuSign SA Client components**.**
6. When installation is complete, a success message appears. Click **Finish.**

Uninstalling the DocuSign SA Administrative Client

To uninstall the DocuSign SA administrative client:

1. Go to the system Control Panel and activate the **Uninstall a Program** option.
2. Uninstall the **DocuSign Signature Appliance Client**.

   > ***Note***: Other DocuSign Signature Appliance components will appear in the list of components to uninstall, however, select to uninstall only the **DocuSign Signature Appliance Client**.and this will uninstall all related components.
   >
   > ***Note***: Please ignore the version information displayed in the Control Panel. The installed version appears when running the *Client Configuration* and activating the Help/About option.

3. The following screen appears. Click **Remove** to uninstall. The uninstalling process begins.

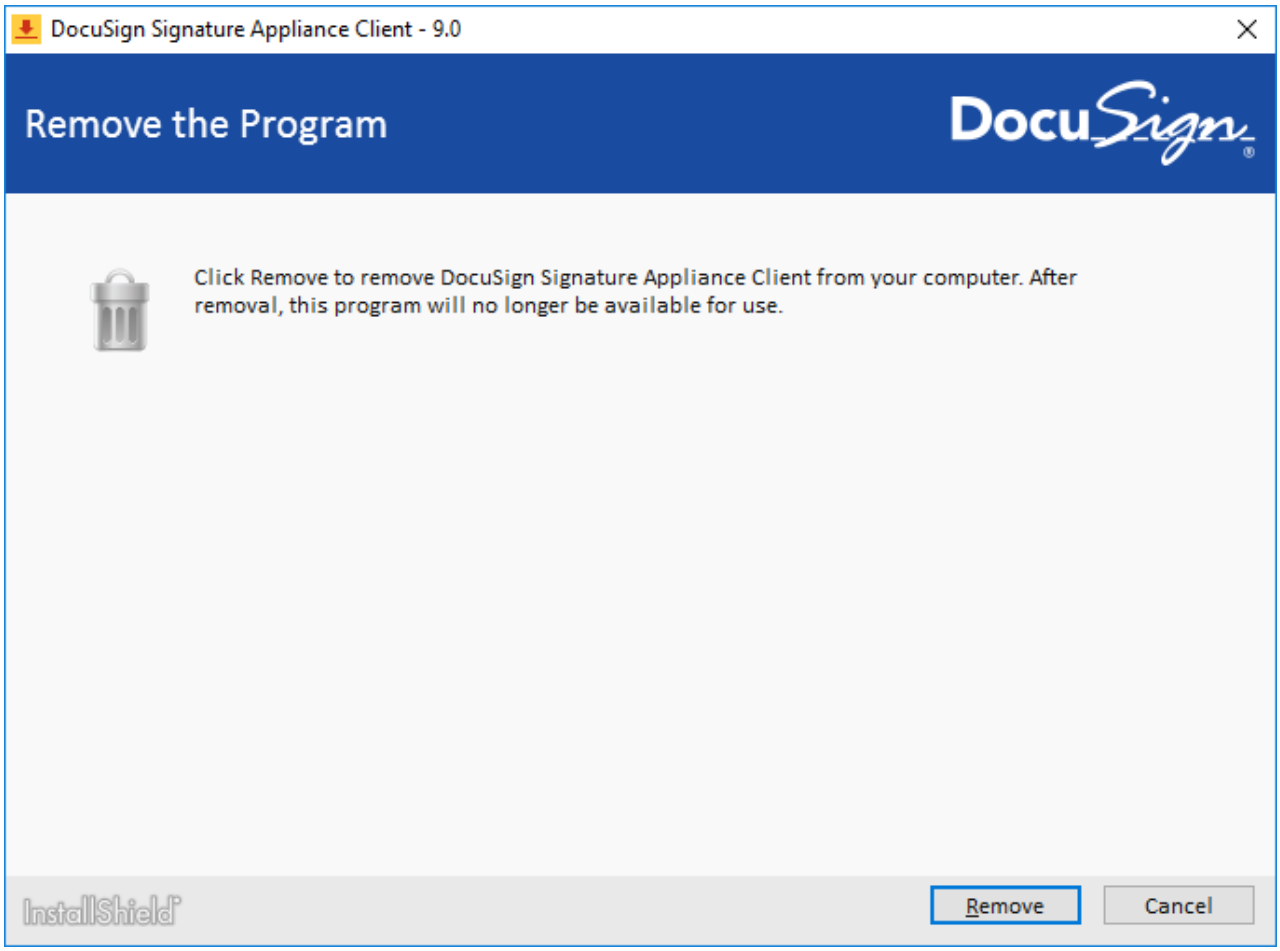


Figure 4 Removing the DocuSign SA Administrative Client

4. When the DocuSign SA Administrative Client is uninstalled from the workstation, a screen appears to inform you that the system finished uninstalling. Click **Finish**.

The DocuSign SA 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 SA FIPS Appliance Hardware version 8.0 – refer to *Installing the DocuSign SA FIPS Appliance Hardware 8.0*.
- DocuSign SA Enterprise Appliance Hardware version 8.1 – refer to *Installing the DocuSign SA Enterprise Hardware 8.1*.

Installing the DocuSign SA FIPS Appliance Hardware 8.0

The DocuSign SA FIPS Appliance hardware (shown in Figures 5 and 6) includes:

- A vent for the inner fan.
- Three front panel LEDs – from left to right: Power On/off LED, Tamper/Hard Disk LED and Power Supply Status LED
  - **Power On/Off** LED
    - Constant blue when the Appliance is on
  - **Tamper/Hard Disk** LED
    - Flashing red upon tamper
    - Flashing green upon internal SSD activity
  - **Power** LED
    - Constant green – dual power supply functioning
    - Flashing green – only one power supply functioning
    - Red – power supply problem
- A USB connector for inserting MiniKey tokens.
- A power switch.
- A touch screen for basic console information.
- Dual power supply. Each of the units is connected to a power network. Each unit includes a status LED indicating the status of the power supply unit:
  - Green – This power supply unit is now in use
  - Flashing Green – This power supply unit is on standby. This means that the other power supply unit is now in use
  - Red – This power supply unit has a malfunction
  - Orange – This power supply unit is not attached to power.
- Two Ethernet connectors for connecting to the network.
  - An Ethernet connector for the regular secure interface, marked with the Ethernet MAC Address of the Ethernet Interface.
  - An Ethernet connector dedicated to the Web Console (IP address 10.0.0.2, port 8088), marked **MGMT**.



Figure 5 DocuSign SA FIPS v8.0 hardware Front Panel



Figure 6 DocuSign SA FIPS v.8.0 Back Panel

The following table lists the physical dimensions of the DocuSign SA 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 SA FIPS v8.0 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 DocuSign SA 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 SA 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 Audit 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 DocuSign sales representative.

   Note: The license Minikey token may have an expiration date.
   Refer to *Displaying DocuSign Signature Appliance Status* for instructions on how to view the expiration date.
   Refer to *Obtaining a New DocuSign SA License* for instructions on how to obtain an updated license.

   Note: If the maximum number of end-users allowed by the license MiniKey token is less than the number of users in the database, the Appliance will not start properly. Please contact DocuSign for an updated license token.

   - A physical key for front panel locking.

2. The DocuSign SA FIPS box is rack mountable. Install DocuSign SA 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 SA FIPS box on the shelf.
   - Use a screw driver, 4 screws, 4 washers, and 4 nuts to secure the DocuSign SA FIPS box to the front vertical rail of the rack.
     Use the four holes in the front of the DocuSign SA 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 SA supports 10/100/1000 Mbits/sec 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 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, you must set the Appliance's network parameters using the console. For more information on using the console, refer to *Chapter 6: Using the DocuSign SA Console*.

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 104ºF 5 to 40ºC	- 4 to 149ºF - 20 to 65ºC
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 SA FIPS/Common Criteria Certificates

The DocuSign SA FIPS Appliance complies with the following certificates:

- UL: Certificate #CU72160723, File# 31680947.001, 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: 2 x 5.8A/2.9A (the 2 x is due to a dual power supply)

    Power dissipation: 250 Watt, 850 BTU/h

    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 2665, 2779.
- Common Criteria EAL4+ validation:

  Certificates appear in the Common Criteria portal at https://www.commoncriteriaportal.org/products/

Warnings



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

Installing the DocuSign SA Enterprise Hardware 8.1

The DocuSign SA Enterprise hardware (shown in Figure 7 and Figure 8) includes:

- Dual power supply.
- A recessed power button on the front panel.
- Two Ethernet connectors (see Figure 8):
  - An Ethernet connector for the regular secure interface, marked **2**.
  - An Ethernet connector dedicated to the Web Console (IP address 10.0.0.2, port 8088), marked **1 (IMM)**
- 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.

Note: The DocuSign SA Enterprise includes two additional LAN interfaces that are not operational and are covered with lids.



Figure 7 DocuSign SA Enterprise Front Panel



Figure 8 Ethernet connectors in DocuSign SA Enterprise Hardware version 8.1 Back Panel

The following table lists the dimensions of the DocuSign SA Enterprise hardware version 8.1 (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 SA Enterprise 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 SA Enterprise 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 SA Enterprise model. If the license MiniKey token is not inserted, the Appliance automatically shuts down after two hours. In this case, the Audit 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 SA Enterprise Appliance. If you require additional user licenses, contact your DocuSign sales representative.

   Note: If the maximum number of end-users allowed by the license MiniKey token is less than the number of users in the database, the Appliance will not start properly. Please contact DocuSign for an updated license token.
2. Connect the power cable to the DocuSign SA 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 SA Enterprise supports 10/100/1000 Mbits/sec Ethernet connections.

   Caution: Use shielded network cables.
4. On the DHCP server, you can set up a specific IP address for the DocuSign SA Enterprise 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 SA Enterprise. For more information on using the console, refer to *Chapter 6: Using the DocuSign SA Console*.
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 95ºF 10 to 35ºC	-40 to 140ºF -40 to 60ºC
Relative Humidity	8 to 80 % (non-condensing)	8 to 80 % (non-condensing)

***Caution*:** Make sure that the temperature inside the rack does not exceed 35ºC / 95ºF.

Installing the DocuSign Signature Appliance Software

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

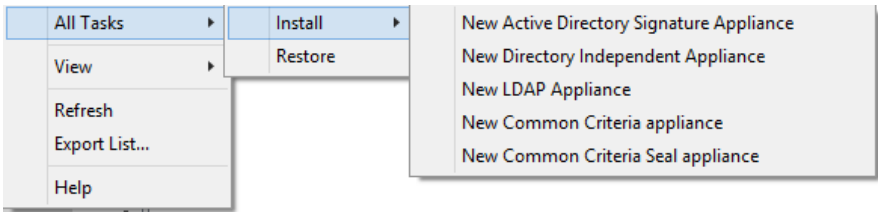


Figure 9 DocuSign SA Installation Options

If you are planning on *Using DocuSign SA in Manual External CA Mode*, then:

- If you plan to use Symantec as the external CA, you must create a Symantec profile before installing DocuSign SA, Refer to *Creating a Symantec Profile Preparatory to Configuring Symantec as DocuSign SA's External CA*.
- If you plan to use DocuSign CA as the external CA, please contact DocuSign Support.
- If you plan to use DocuSign TSCP as the external CA, this will require many initial and ongoing procedures handled by the organization and the organization's employees/users. One of the major requirements is an employee/user identification process handled by a trusted role. As part of the employee/user onboarding process, the employee/user will be required to sign a DocuSign envelope.
  A similar envelope will need to be signed if the employee's email or his/her common name has changed.
- Using Comodo as the external CA is not supported any more.

***Note**:* The following software installation instructions apply for all DocuSign SA hardware models, unless otherwise noted.

***Note**:* Starting from DocuSign SA version 8.2, an additional entry for installing a *New Common Criteria Seal appliance* option appears for installing DocuSign SA as a Seal Creation Device.

Installing DocuSign SA in a Microsoft Active Directory Environment

The DocuSign SA 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 SA since DocuSign SA can be instructed to automatically synchronize with the users located in the Microsoft Active Directory. Depending on DocuSign SA'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 SA 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 be 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 DocuSign SA Root CA certificate is published at the Microsoft Active Directory as well.
- *Users* – When using active directory, DocuSign SA 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 SA 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 SA's domain.
In this mode of work, users' synchronization works differently: upon first access of a new user, DocuSign SA 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 SA, and his/her certificate is revoked.

In order to manage DocuSign SA after installation, you must be either a member of the administrators group and be a valid DocuSign SA 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 SA 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 DocuSign Signature Appliances Management application. In this installation scenario, the administrator logged on to the

administration workstation that is running the DocuSign SA 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 SA serves only certain organizational units. This type of installation requires performing certain preparations prior to installing DocuSign SA, as well as performing certain actions after DocuSign SA was installed.
  Refer to *Appendix A: DocuSign SA Installation with Reduced Privileges* for detailed information on how to install DocuSign SA 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.

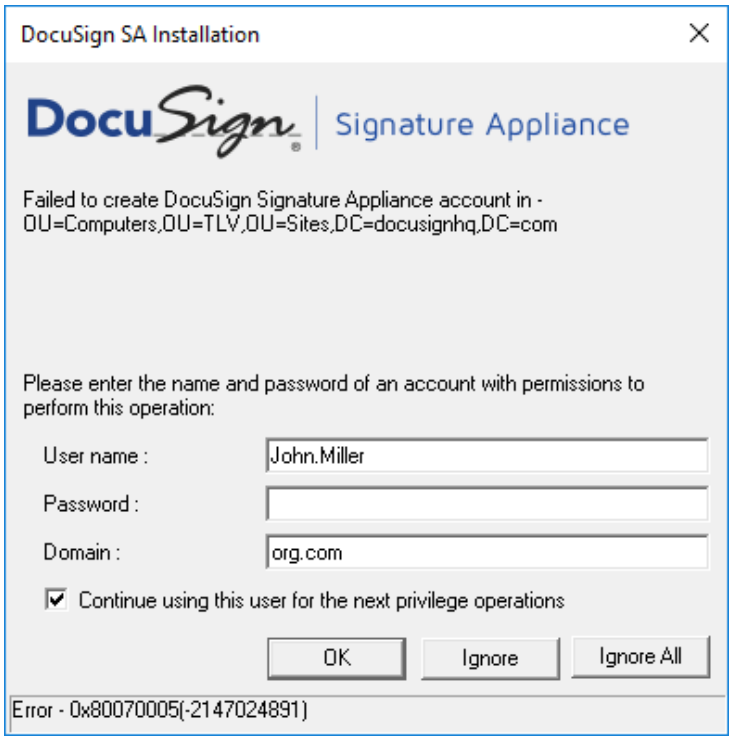


Figure 10 Switching to a Different Administrator

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 SA 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 DocuSign SA CA certificate and the DocuSign SA 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 SA software:

1. In the system tray, right-click the icon and select **Administrative Tools → Appliances Management**. The *DocuSign Signature Appliance Management* window appears.
2. Right-click **Signature Appliances** and select **All Tasks → Install → New Active Directory Signature Appliance**. The DocuSign SA License Agreement appears.
3. Accept the license agreement and click **Next**. The *Network Setup* dialog box appears.

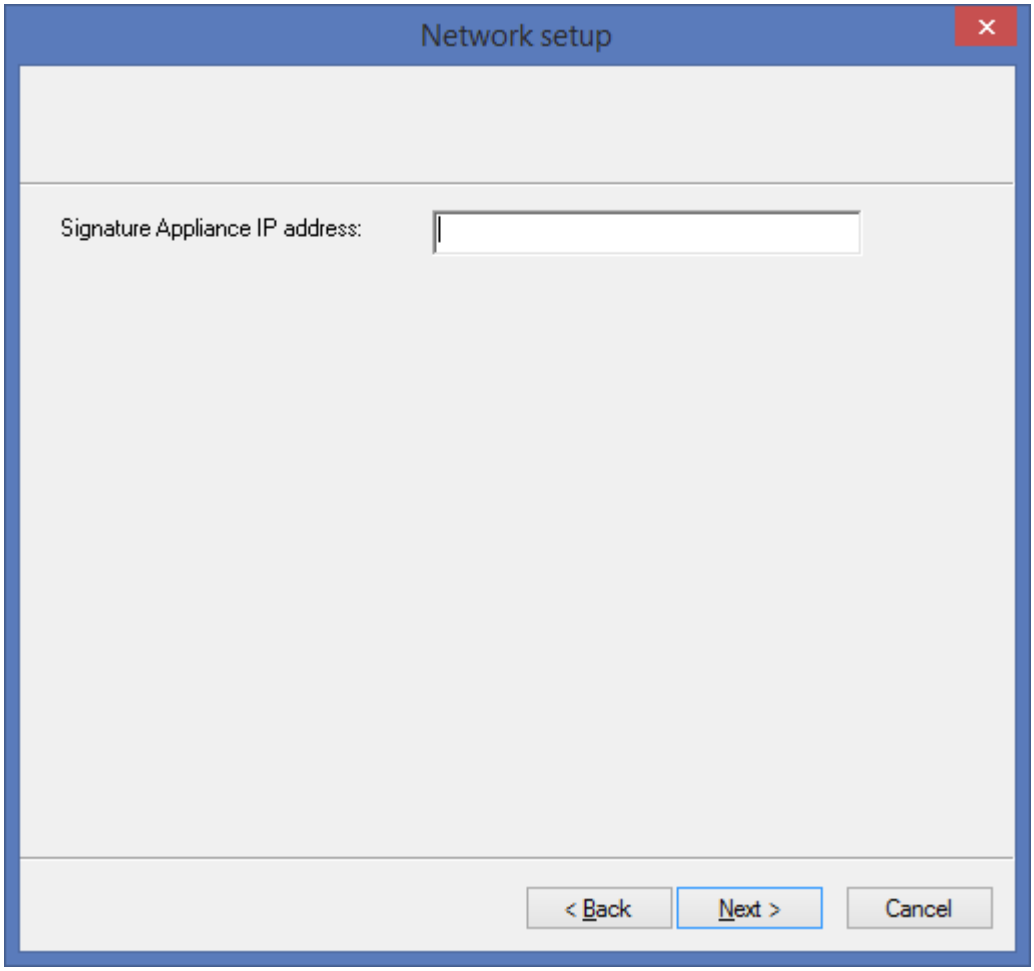


Figure 11 Network Setup Dialog Box

4. 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 SA hardware version 8.0, IPv6 is also supported. You can enter an IPv6-type IP address in the **DocuSign Signature Appliance IP address** field.

Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to *Setting the Appliance IP Address*.

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 SA (refer to *Setting the Appliance IP Address*.

5. Click **Next**. The DocuSign SA Administrator User dialog box appears.

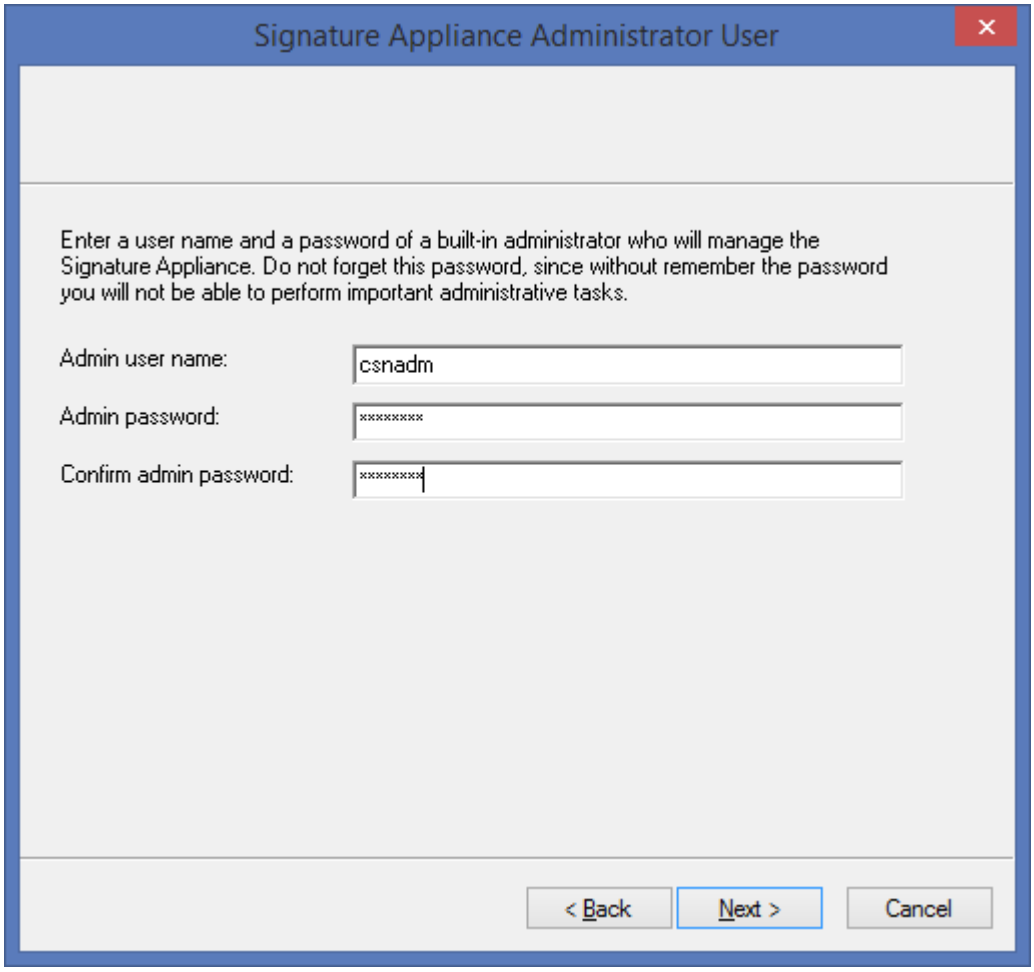


Figure 12 DocuSign SA Administrator User Dialog Box

6. 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 SA.

> ***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 SA 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.

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

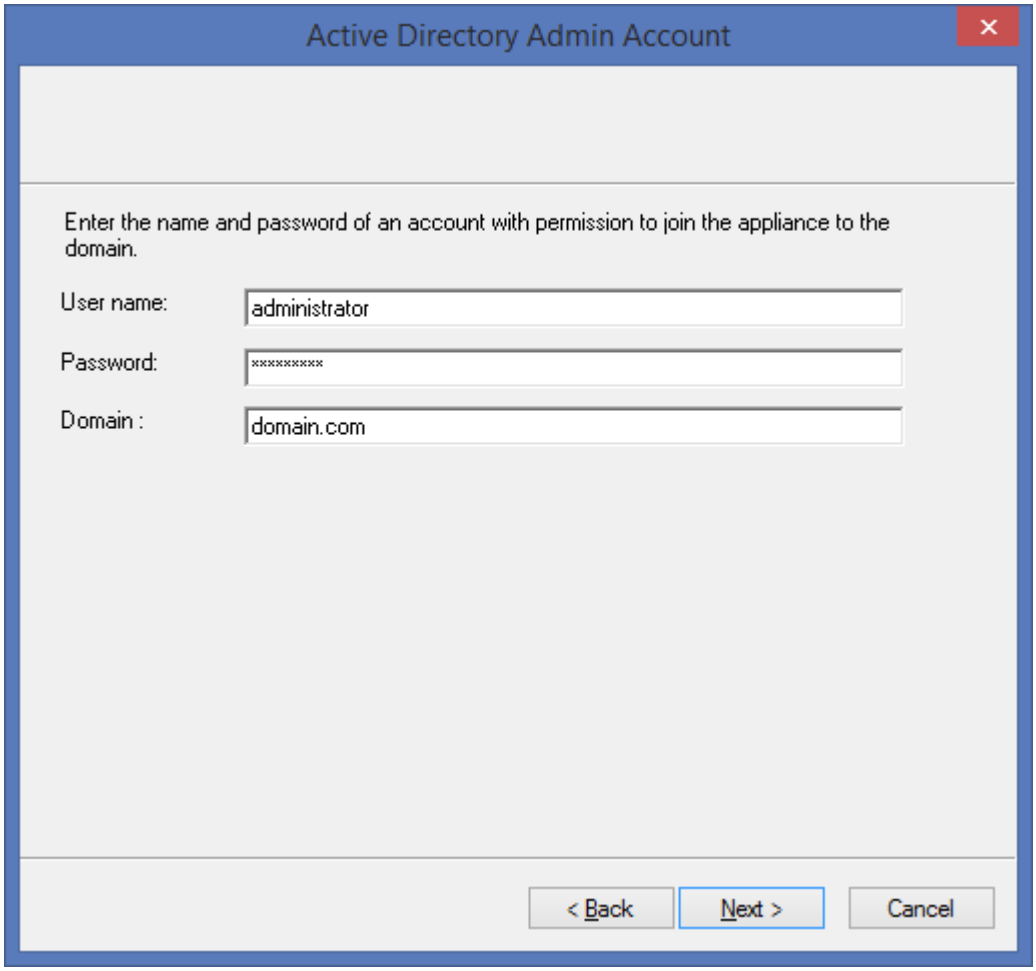


Figure 13 Active Directory Admin Account Dialog Box

> ***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*).

8. Enter an administrative account that has permission to join the DocuSign Signature Appliance to the Domain.

9. Click **Next**. The *Directory Setup* dialog box appears.

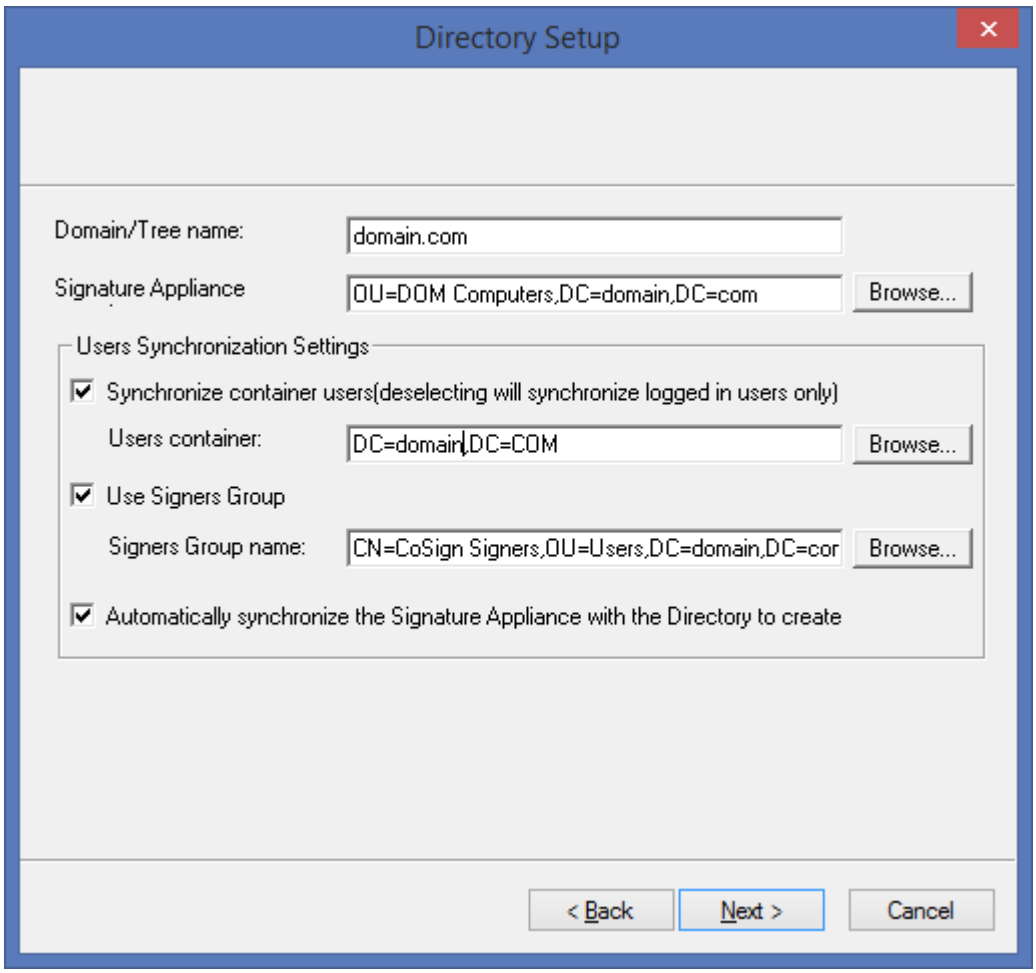


Figure 14 Directory Setup Dialog Box

> ***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 SA 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.

10. Enter the following information:

- **Domain/Tree name** – The name of the domain that contains the DocuSign Signature Appliance.
- **DocuSign SA 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.

Note: If the DocuSign SA 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 SA 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 SA 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 SA users. Note that in the Signers group it is possible to define additional subgroups to ease the selection of DocuSign SA 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 SA, 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.
- **Use Signers Group** – Select this option to specify that only users who belong to the Signers group be defined as DocuSign SA 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.
- **Automatically synchronize the Signature Appliance with the directory to create user database** – If this option is selected, DocuSign SA 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 SA administrator, you can define additional DocuSign SA administrators who are valid Active Directory users. If you do so, the DocuSign SA administrator must also be located in this subtree and the Signers Group in order to be a valid DocuSign SA user. Otherwise the administrator will not be able to administrate DocuSign SA.

Important: In the case of a regular AD installation, do not modify the name of the sub-tree of DocuSign SA 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 SA OU (DocuSign SA 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 SA. 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 SA (i.e., email address), the user will be updated in DocuSign SA as well.
- If the user is deleted from the domain, the user will be deleted from DocuSign SA as well and his/her certificate will be revoked.

11. 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 SA users are created only after assigning users to the Signers group.

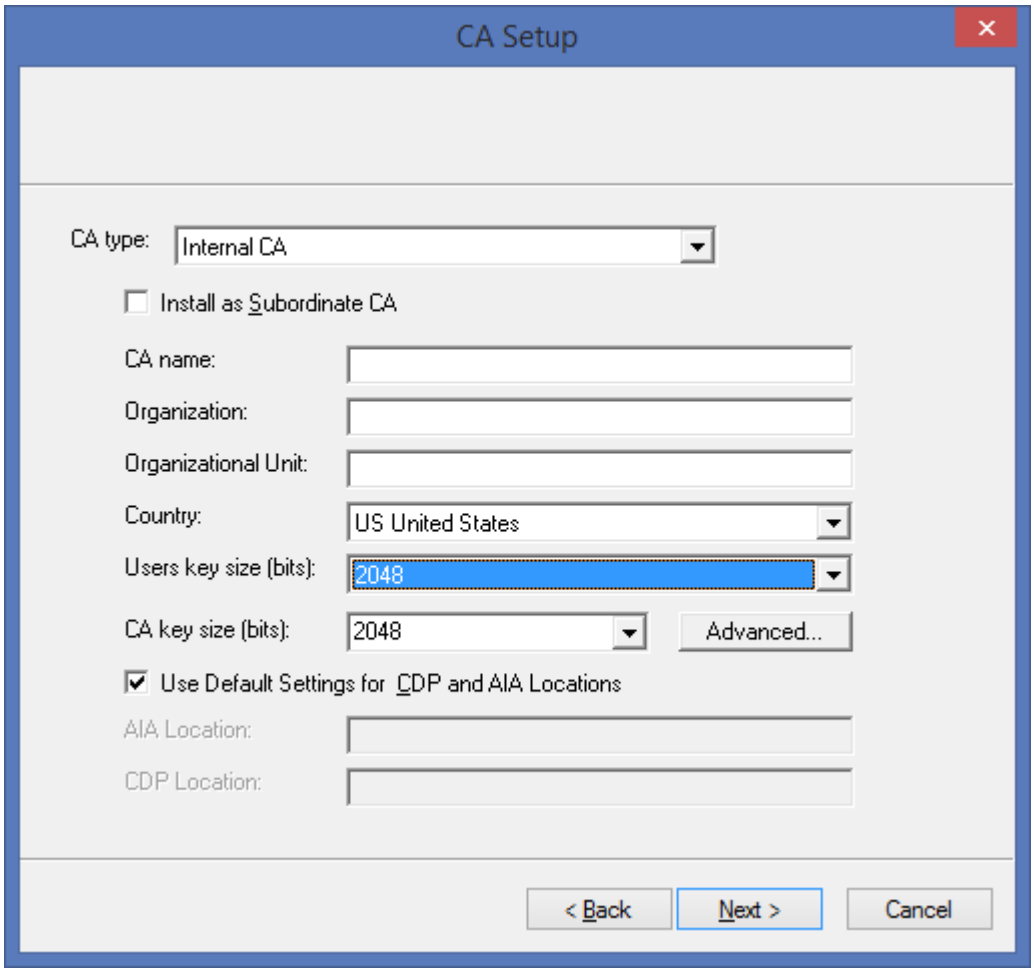


Figure 15 CA Setup Dialog Box

- 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 8.
- If you want the DocuSign Signature Appliance to use an external Certification Authority (CA) for automatically generating end-user certificates, refer to *Using an External CA in Automated Mode* for detailed explanations of the *CA Setup* dialog box. After configuring the **CA *type*** in the *CA Setup* dialog box, continue with Step 8.
- 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 SA in manual external CA mode. It is highly recommended to read the section *Using DocuSign SA in Manual External CA Mode* before installing DocuSign SA with this option.

12. Click **Next**. The DocuSign SA 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 DocuSign SA Administration MMC display.

13. At the **`Please insert a backup Minikey`** prompt, insert the first backup MiniKey token.
14. 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.
15. 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 SA as a Subordinate CA*.

    If you selected the **CA Type** to be **Symantec World Wide Verifiable CA** in the *CA Setup* dialog box, some additional configuration is required, as described in *Using an External CA in Automated Mode – Symantec*.

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

    If you did not select **Automatically synchronize DocuSign SA 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.
16. 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 SA 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).
17. In the DocuSign SA Administration MMC window, right-click **DocuSign Signature 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 SA using the DocuSign SA 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 DocuSign 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 DocuSign Signature Appliance Status* for instructions on how to view the expiration date. Contact DocuSign for a replacement license MiniKey token before the current key expires.

Note: If the maximum number of end-users allowed by the license MiniKey token is less than the number of users in the database, the Appliance will not start properly. Please contact DocuSign for an updated license token.

Note: In a high availability environment, the licenses of all the DocuSign Signature Appliances in the high availability site should have identical limitations on the number of appliance users and license expiration date.
The limitation on the amount of transactions per year should also be the identical.

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 SA's database to safely recover and restore DocuSign SA data. For more information on how to backup and restore the DocuSign SA's database, refer to *Backing up the DocuSign SA 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 a 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 SA operation. The table also describes the actions and permissions of each of these users.
For more information on how DocuSign SA interfaces with Active Directory, refer to *Appendix A: DocuSign SA Installation with Reduced Privileges*.

Table 1 Users Involved in the Installation and Operation of DocuSign SA

User	Actions	Active Directory Operations	Permissions	Suggested Permission Group
Domain Administrator	Running the DocuSign SA Administration 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 SA Administrator	Performing DocuSign SA 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 SA 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 SA generates a new account for the user and depending on the DocuSign SA 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-082035.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 DocuSign SA models, unless otherwise noted.

You install the DocuSign Signature Appliance software from the DocuSign SA Administration MMC. In order to manage DocuSign SA 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 SA software:

1. In the system tray, right-click the  icon and select **Administrative Tools → Appliances Management** (Figure 53). The DocuSign Signature Appliance Management window appears.

2. Right-click **DocuSign Signature Appliances** and select **All Tasks → Install → New LDAP appliance**. The DocuSign SA License Agreement appears.
3. Accept the license agreement and click **Next**. The Network Setup dialog box appears.

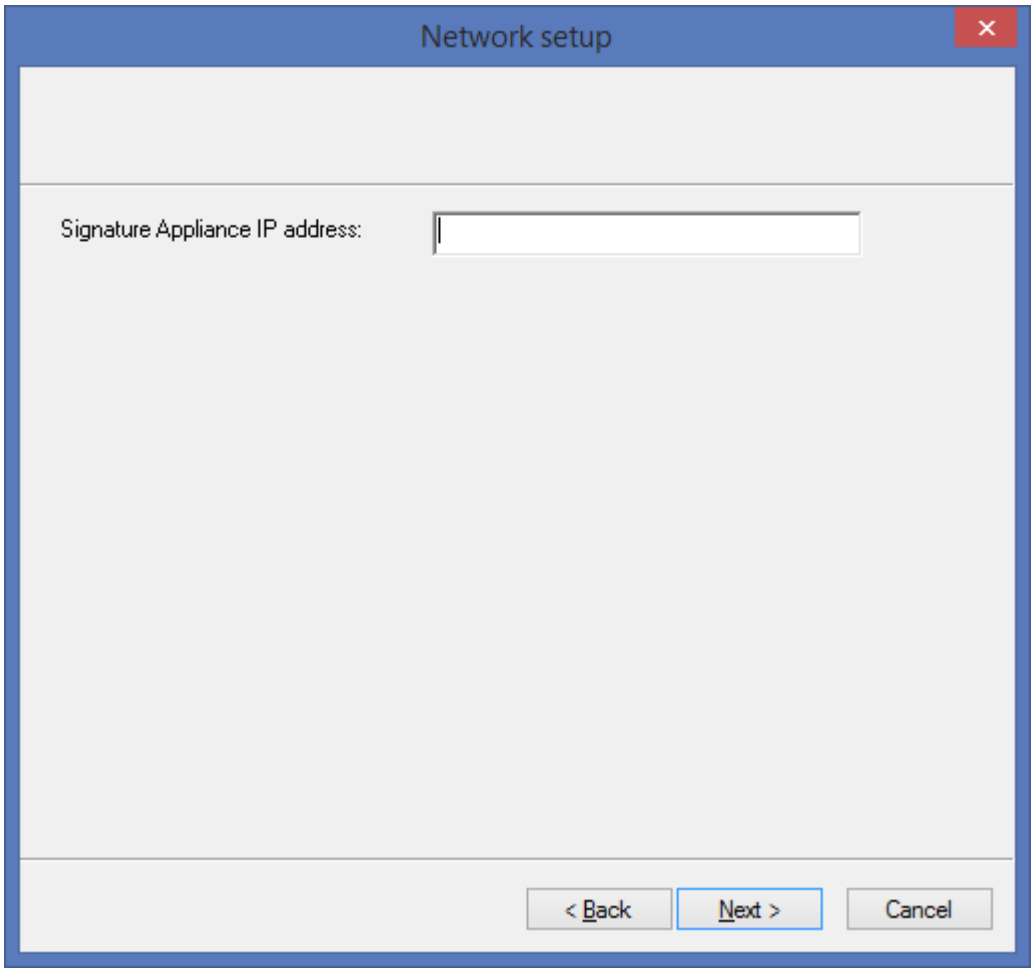


Figure 16 Network Setup Dialog Box

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

   Note: For information on setting up the IP address of the DocuSign Signature Appliance refer to *Setting the Appliance IP Address*.

5. Click **Next**. The DocuSign SA administrator user dialog box appears.

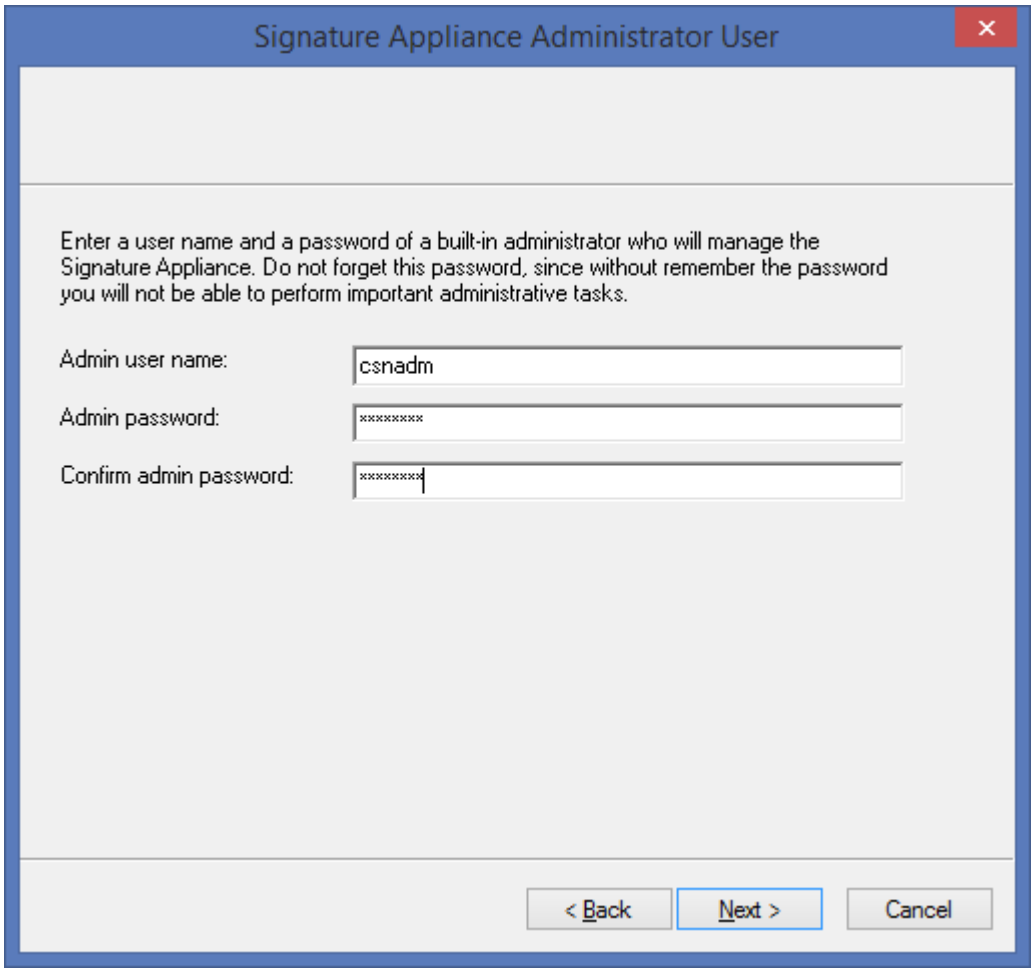


Figure 17 DocuSign SA Administrator User Dialog Box

6. 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 SA.

   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 SA 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.

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

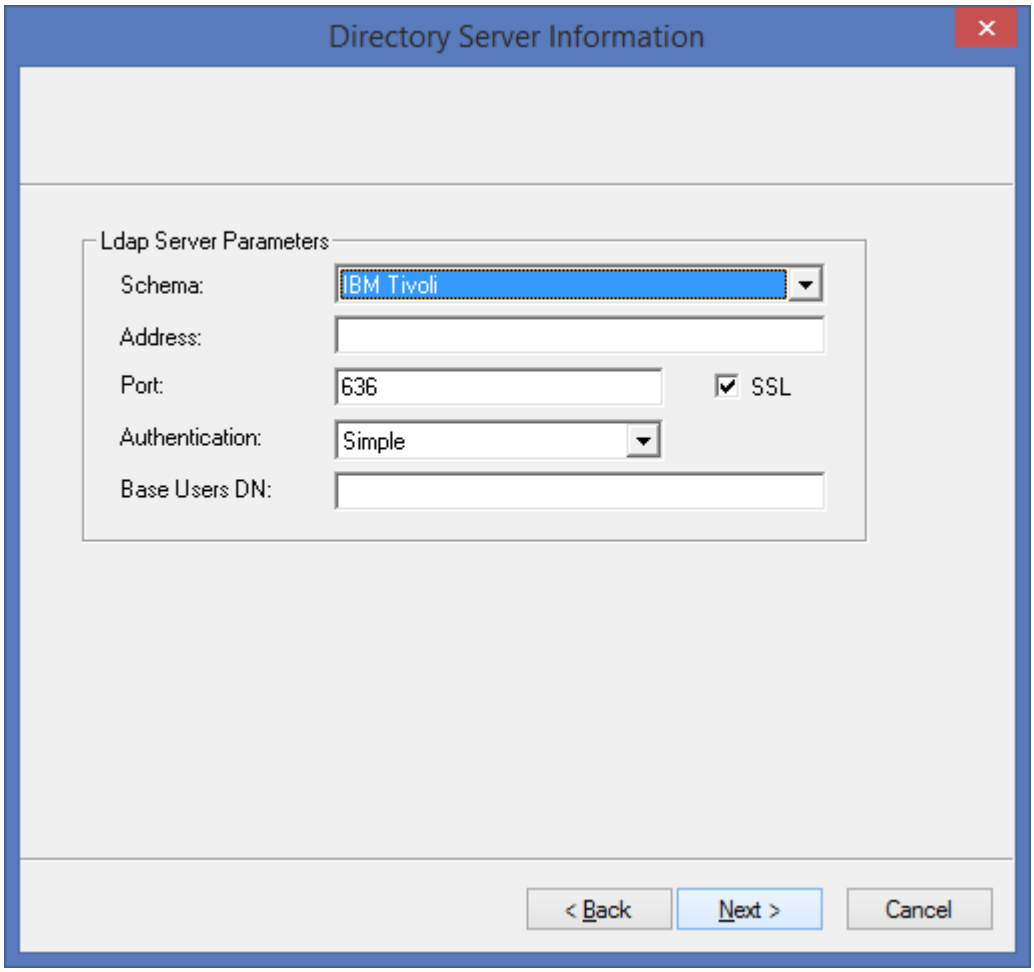


Figure 18 Directory Server Information Dialog Box

8. Enter the following information:

- **Schema –** The commercial name of the LDAP server. This parameter directs DocuSign SA 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 SA.

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

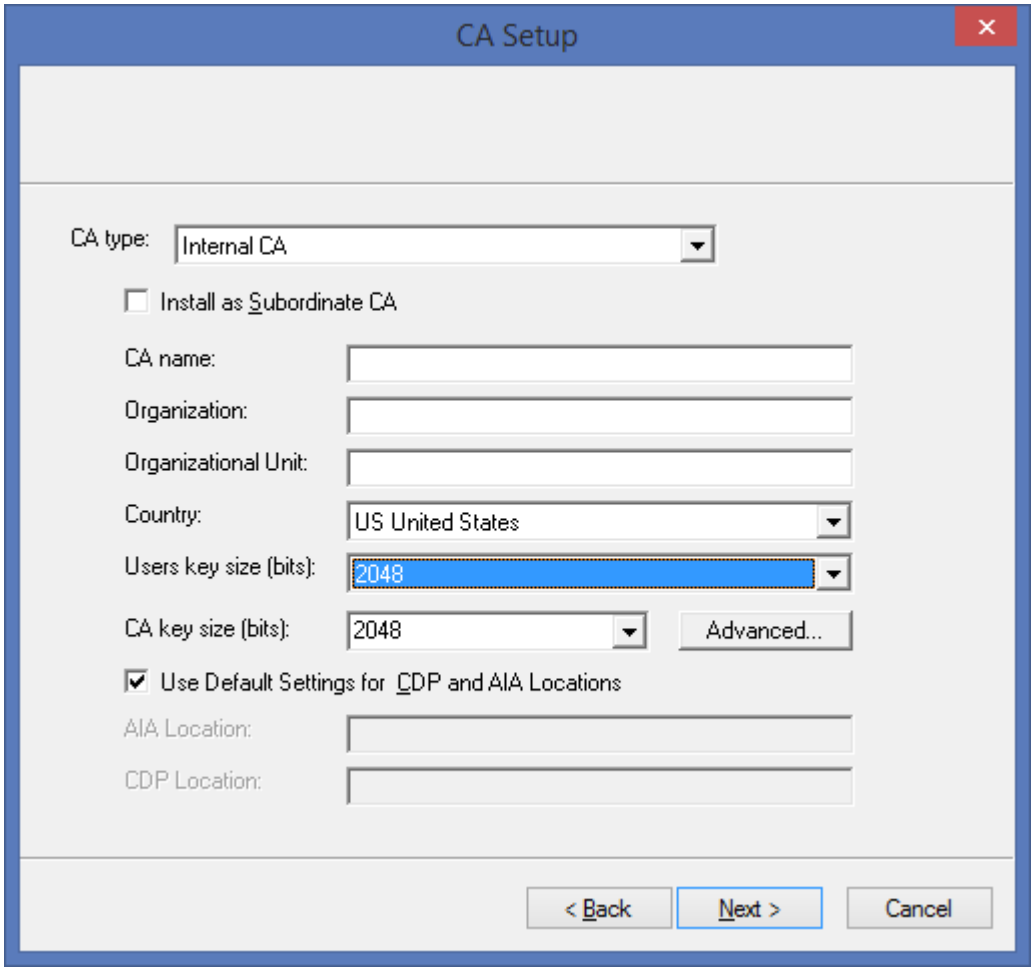


Figure 19 CA Setup Dialog Box

- 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 *10*.
- If you want the DocuSign Signature Appliance to use an External Certification Authority (CA) for automatically generating end-user certificates, refer to *Using an External CA in Automated Mode* for detailed explanations of the *CA Setup* dialog box. After configuring the **CA Type** in the *CA Setup* dialog box, continue with Step *10*.
- 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 SA in Manual External CA Mode* before installing DocuSign SA with this option.

10. Click **Next**. DocuSign SA 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 the Enterprise model) and the DocuSign SA Administration MMC display.

11. At the **`Please insert a backup Minikey`** prompt, insert the first backup MiniKey token.
12. 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.
13. 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 SA as a Subordinate CA*.

    If you selected the **CA Type** to be **Symantec World Wide Verifiable CA** in the *CA Setup* dialog box, some additional configuration is required, as described in *Using an External CA in Automated Mode – Symantec*.

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

    If you are installing an Alternate Appliance do not press **Cancel**, since this will cause the Appliance not to be installed correctly, and you will need to re-install it
15. In the DocuSign SA Administration MMC window, right-click **DocuSign Signature Appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You can now manage DocuSign SA using the DocuSign SA 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 DocuSign 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 DocuSign Signature Appliance Status* for instructions on how to view the expiration date. Contact DocuSign for a replacement license MiniKey token before the current key expires.

Note: If the maximum number of end-users allowed by the license MiniKey token is less than the number of users in the database, the Appliance will not start properly. Please contact DocuSign for an updated license token.

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 and license expiration date.
The limitation on the amount of transactions per year should also be the identical.

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 SA's database to safely recover and restore DocuSign SA data. For more information on how to backup and restore the DocuSign SA's database, refer to *Backing up the DocuSign SA 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 a 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 SA 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 SA to access the LDAP based directory. Connect to the appliance administration using the local DocuSign SA administrative account.
Fill in the parameters **LDAP DocuSign SA User Name** and **LDAP DocuSign SA User Password** with an administrative account that can perform queries to the directory**.** For more information, refer to *LDAP* in *Changing DocuSign SA System Parameters*.

Installing DocuSign SA in a Directory Independent Environment

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

- DocuSign SA 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 SA provides external signature APIs that enable the integrator to insert a user into DocuSign SA 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 SA signature APIs. For information, refer to the *DocuSign SA Signature APIs Developer's Guide*.
- DocuSign SA is integrated into a product with no user management capabilities. In these cases, the administrator will use a DocuSign SA GUI utility to manage the internal DocuSign SA users. Refer to *Using the Users Management Utility*.

To install the DocuSign SA software:

1. In the system tray, right-click the  icon and select **Administrative Tools → Appliances Management**. The *DocuSign Signature Appliance Management* window appears.
2. Right-click **DocuSign Signature Appliances** and select **All Tasks → Install → New Directory Independent appliance**. The DocuSign SA License Agreement appears.
3. Accept the license agreement and click **Next**. The *Network Setup* dialog box appears.

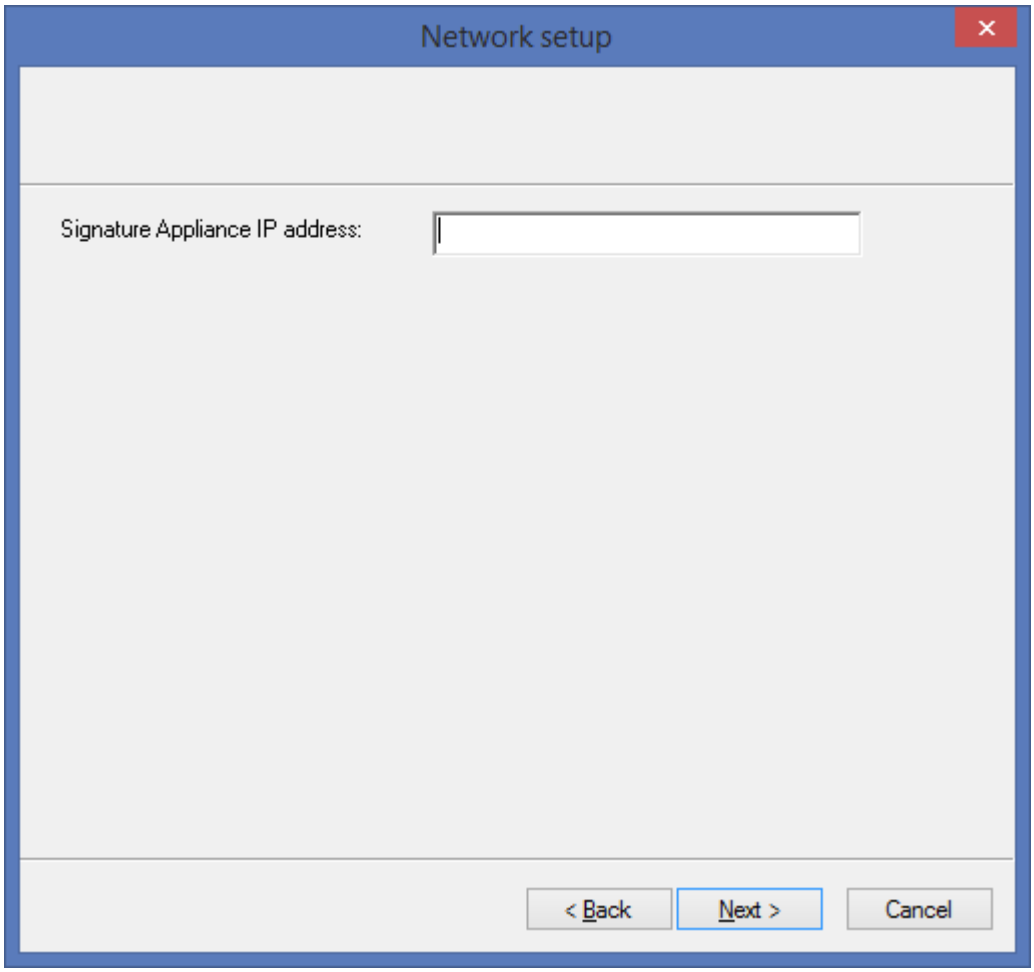


Figure 20 Network Setup Dialog Box

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

   Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to *Setting the Appliance IP Address*.

5. Click **Next**. The *DocuSign SA Administrator User* dialog box appears.

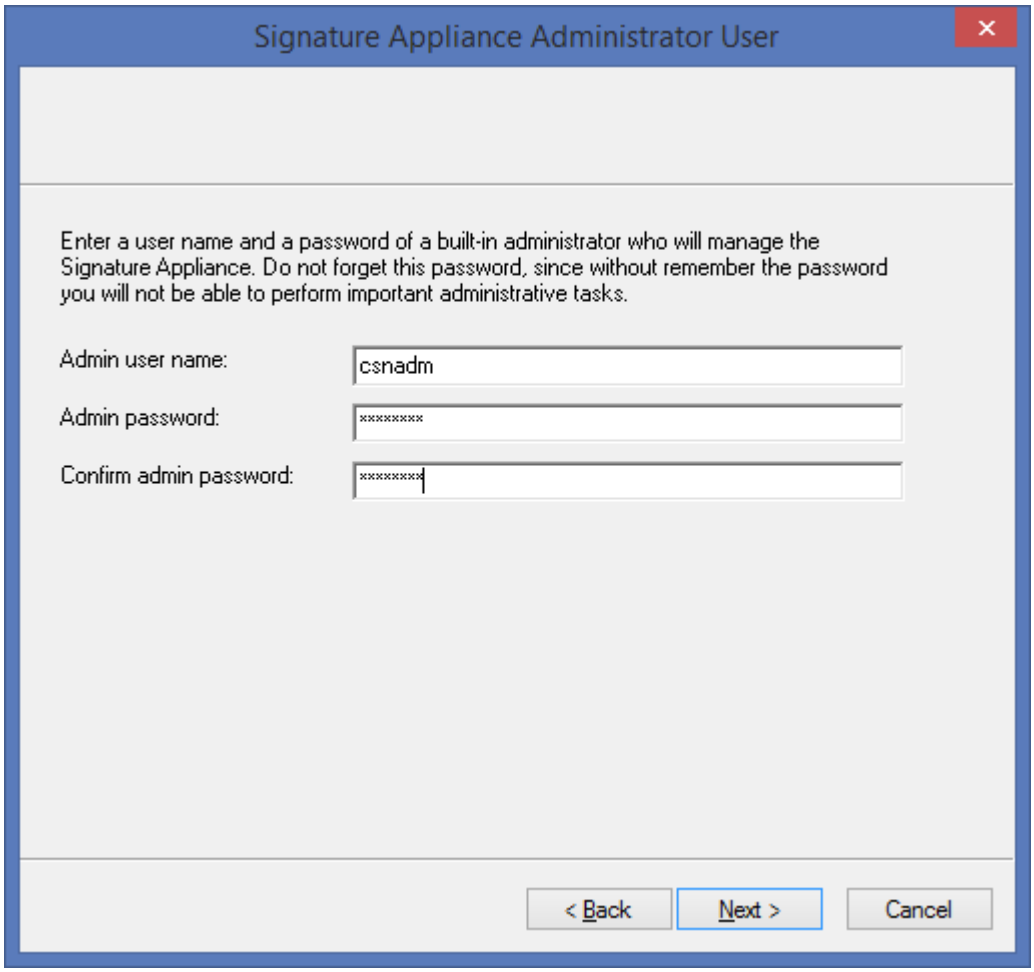


Figure 21 DocuSign SA Administrator User Dialog Box

6. Enter the **DocuSign SA 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 SA with this user name and password.

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

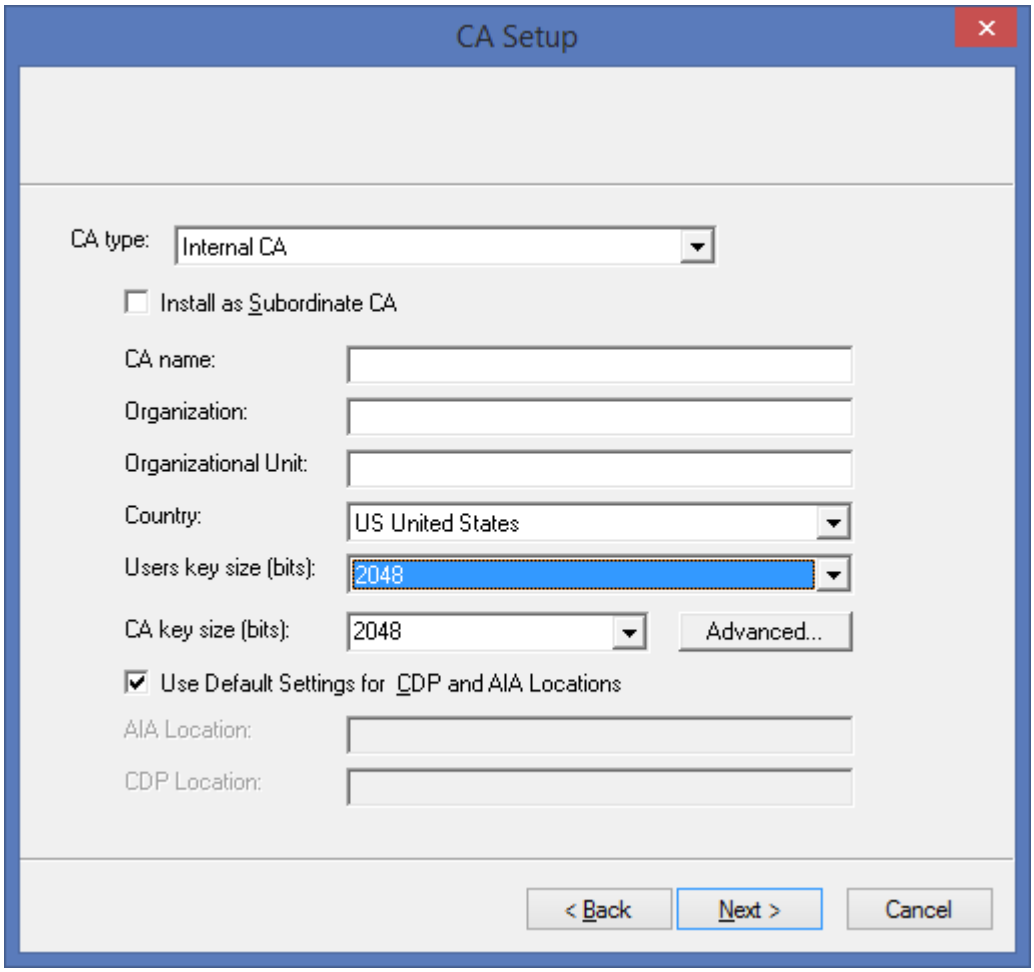


Figure 22 CA Setup Dialog Box

- 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 8.
- If you want the DocuSign Signature Appliance to use an External Certification Authority (CA) for automatically generating end-user certificates, refer to *Using an External CA in Automated Mode* for detailed explanations of the *CA Setup* dialog box. After configuring the **CA Type** in the *CA Setup* dialog box, continue with Step 8.
- 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 SA in Manual External CA Mode* before installing DocuSign SA with this option.

8. Click **Next.** DocuSign SA 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 the Enterprise model) and the DocuSign SA Administration MMC display.

9. At the **`Please insert a backup Minikey`** prompt, insert the first backup MiniKey token.
10. 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.
11. 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 SA as a Subordinate CA*.

    If you selected the **CA Type** to be **Symantec World Wide Verifiable CA** in the *CA Setup* dialog box, some additional configuration is required, as described in *Using an External CA in Automated Mode – Symantec*.

    In all other cases, your part in the installation is complete.
12. 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 SA 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).
>
> If you are installing an Alternate Appliance do not press **Cancel**, since this will cause the Appliance not to be installed correctly, and you will need to re-install it

13. In the DocuSign SA Administration MMC window, right-click **DocuSign Signature Appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You can now manage DocuSign SA using the DocuSign SA Administration MMC (refer to *Chapter 5: Managing the DocuSign Signature Appliance*).
14. Activate the DocuSign Signature Appliance `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 SA users can connect to DocuSign SA 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 DocuSign 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 DocuSign Signature Appliance Status* for instructions on how to view the expiration date. Contact DocuSign for a replacement license MiniKey token before the current key expires.

Note: If the maximum number of end-users allowed by the license MiniKey token is less than the number of users in the database, the Appliance will not start properly. Please contact DocuSign for an updated license token.

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. and license expiration date.
The limitation on the amount of transactions per year should also be the identical.

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 SA's database to safely recover and restore DocuSign SA data. For more information on how to backup and restore the DocuSign SA's database, refer to *Backing up the DocuSign SA 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 a 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 SA in a Common Criteria EAL4+ Mode as a Signature Creation Device or Seal Creation Device

When DocuSign SA is deployed in a Common Criteria mode, special consideration should be given to the security of the DocuSign Signature Appliance's operational environment. For more information, refer to the DocuSign SA Security Target, located in the *Products for Digital Signature* section in the Common Criteria portal (https://www.commoncriteriaportal.org/products/).

In addition, make sure all security measures related to the networking infrastructure of the environment are taken. Make sure that routers, switches, firewalls, etc. are deployed correctly and only allowed requests are sent to or from a deployed DocuSign Signature Appliance.

DocuSign SA installation in a Common Criteria EAL4+ mode is similar to installing DocuSign SA in a Directory Independent mode.

To install the DocuSign SA software:

1. In the system tray, right-click the icon and select **Administrative Tools → Appliances Management**. The *DocuSign Signature Appliance Management* window appears.
2. Right-click **DocuSign Signature Appliances** and select **All Tasks → Install → New Common Criteria appliance**. The DocuSign SA License Agreement appears.
3. Accept the license agreement and click **Next**. The Network Setup dialog box appears.

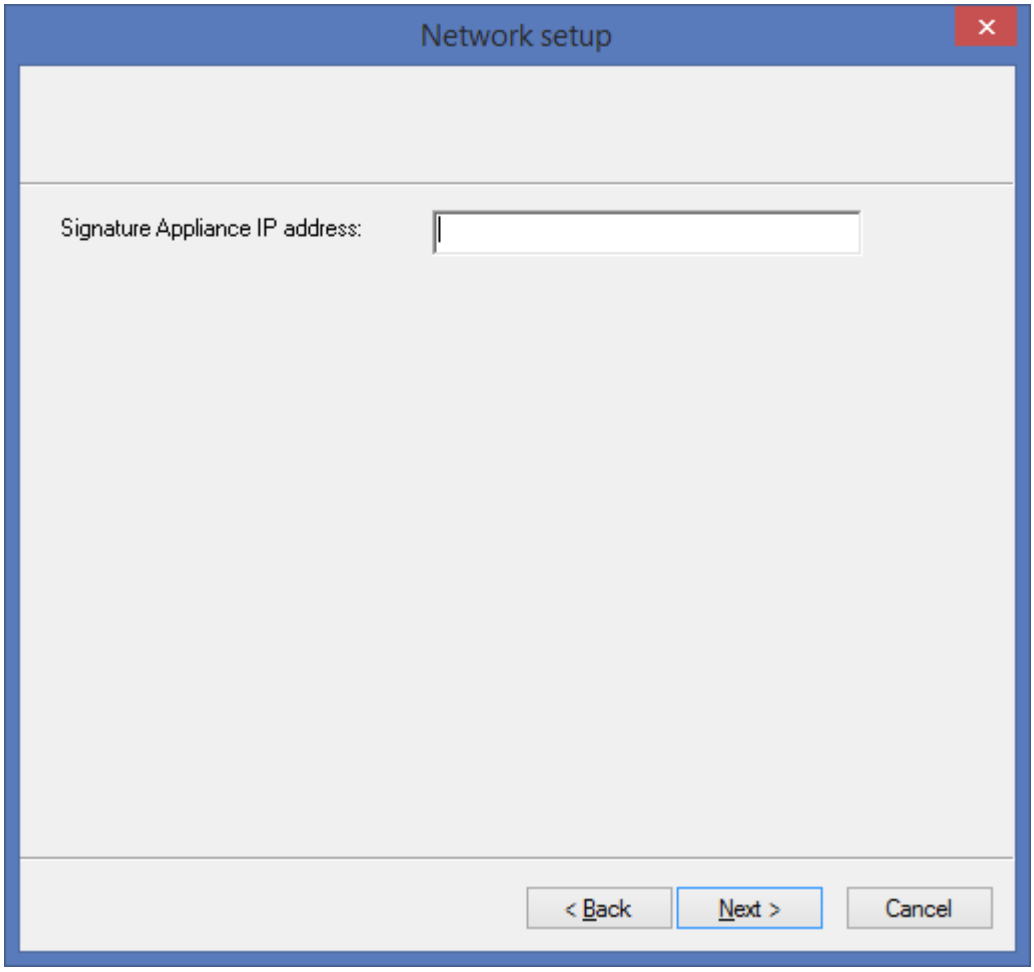


Figure 23 Network Setup Dialog Box

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

   Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to *Setting the Appliance IP Address*.

5. Click **Next**. The *DocuSign SA Administrator User* dialog box appears.

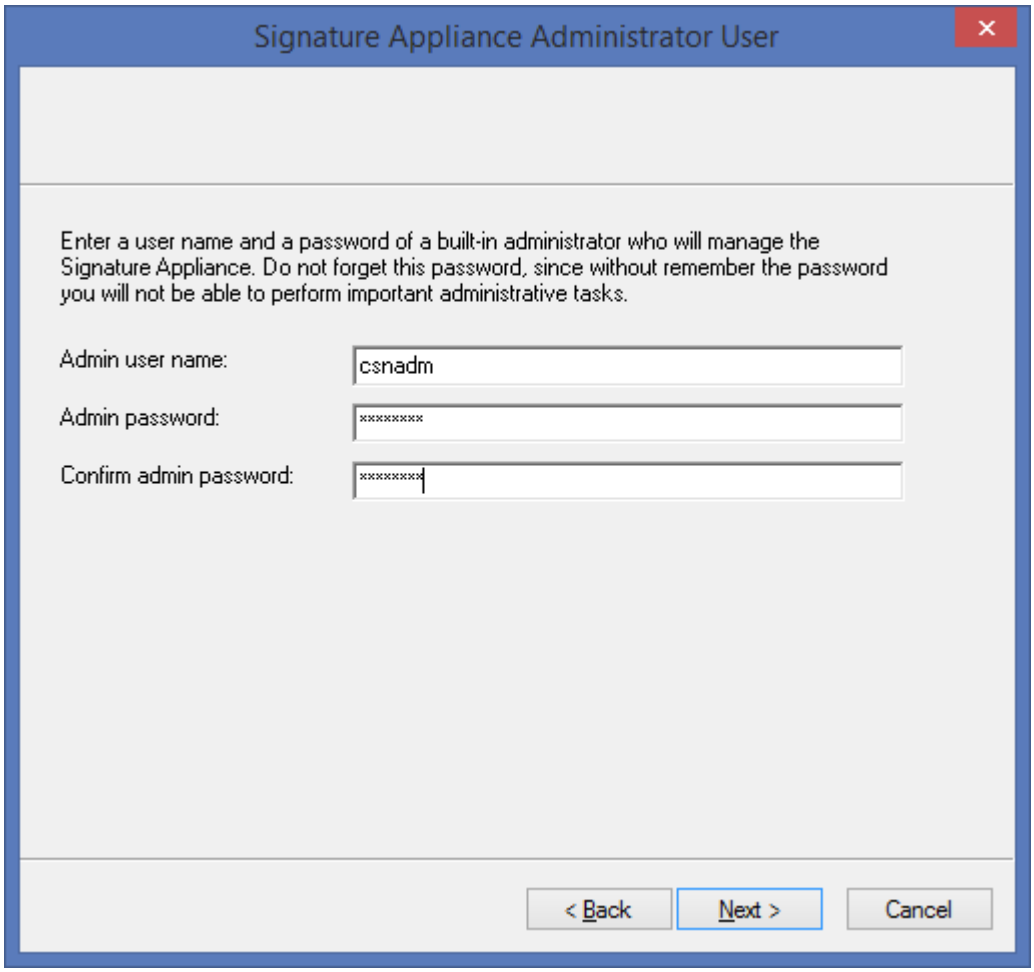


Figure 24 DocuSign SA Administrator User Dialog Box

6. Enter the **DocuSign SA 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 SA with this user name and password.

7. Click **Next.** DocuSign SA 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 DocuSign SA Administration MMC display.

8. At the **`Please insert a backup Minikey`** prompt, insert the first backup MiniKey token.

9. 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.

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

    Your part in the installation is complete.

11. 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 SA 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).
>
> If you are installing an Alternate Appliance do not press **Cancel**, since this will cause the Appliance not to be installed correctly, and you will need to re-install it

12. In the DocuSign SA Administration MMC window, right-click **DocuSign Signature Appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed appliance. You can now manage DocuSign SA using the DocuSign SA Administration MMC (refer to *Chapter 5: Managing the DocuSign Signature Appliance*).
13. Activate the DocuSign Signature Appliance `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 SA users can connect to DocuSign SA 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 DocuSign 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 DocuSign Signature Appliance Status* for instructions on how to view the expiration date. Contact DocuSign 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:*** If the maximum number of end-users allowed by the license MiniKey token is less than the number of users in the database, the Appliance will not start properly. Please contact DocuSign for an updated license token.

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 DocuSign SA 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.

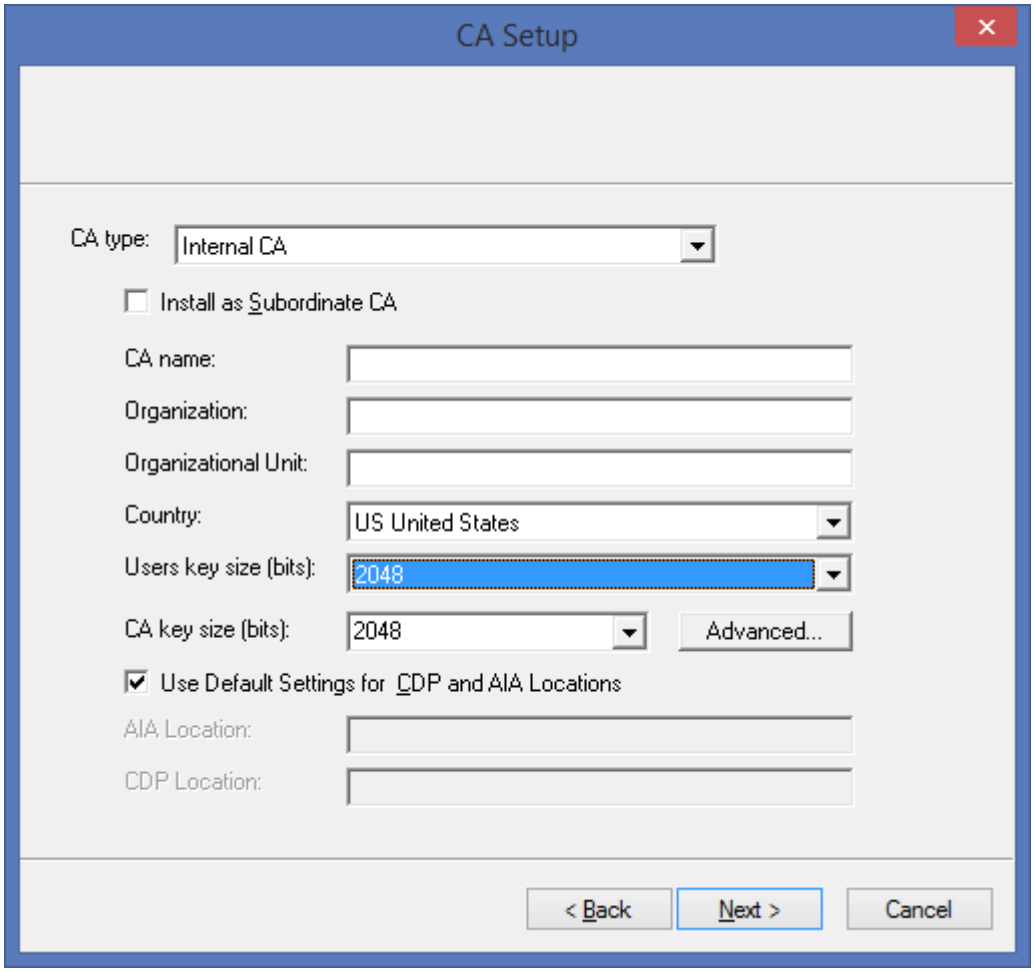


Figure 25 CA Setup Dialog Box

To specify an Internal CA:

1. Specify **Internal CA** in the **CA type** field.
2. Enter the following information:

- **Install as Subordinate CA** – Select this option if you wish to install the DocuSign SA CA as a subordinate CA.
  You can install the DocuSign SA 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 SA 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 SA as a Subordinate CA*.

- **CA name** – The identifying name of DocuSign SA'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 and also in the user 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 and in the user 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.
- **CA key size (bits)** – The size of the key of the CA.
- **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 DocuSign SA 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 SA.
  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 SA installation will also put the DocuSign SA

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 DocuSign SA 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 SA.
  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 SA 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 SA AIA and CRL, refer to *Changing DocuSign SA System Parameters*.

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

- If you are installing DocuSign SA in a Microsoft Active Directory Environment, continue with Step *12*.
- If you are installing DocuSign SA in an LDAP based Environment, continue with Step *10*.
- If you are installing DocuSign SA in a Directory Independent Environment, continue with Step *8*.

Advanced Settings

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

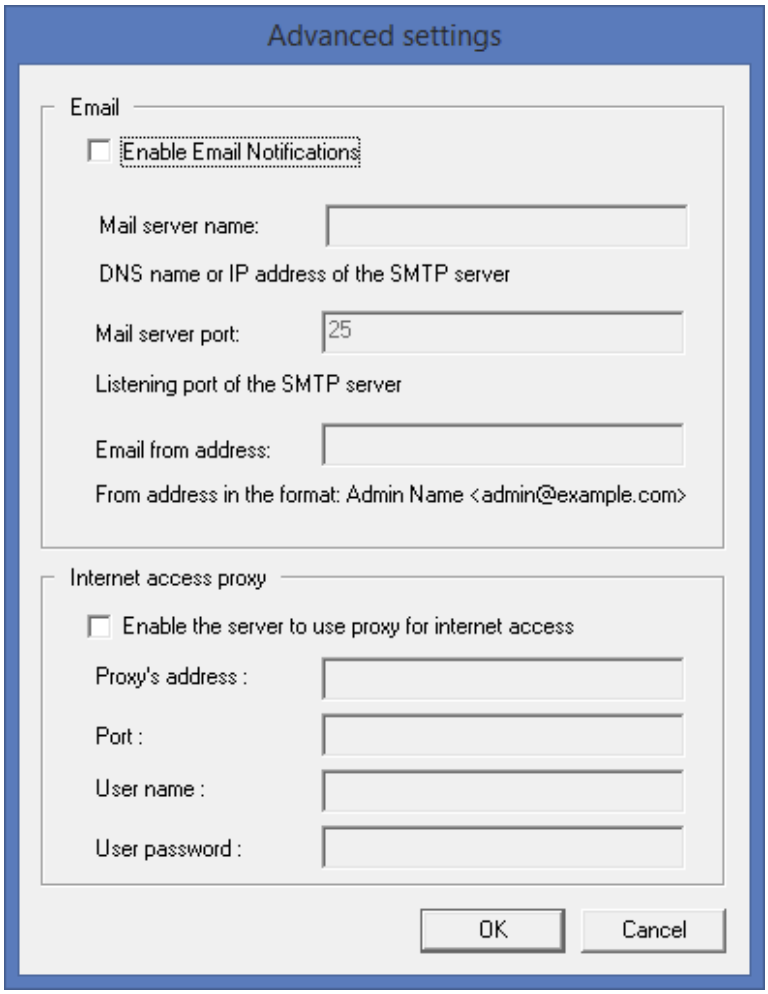


Figure 26 Advanced Settings Dialog Box

- **Enable Email Notification** – Check this option to direct DocuSign SA 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 SA to communicate with the internet through an SSL proxy. This option is relevant for cases where DocuSign SA is configured to use an External 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 SA is installed in Common Criteria EAL4+ mode.

If DocuSign SA 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 DocuSign SA RESTful API.
- During enrollment, a command to generate a key is sent from the DocuSign SA 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 SA 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 DocuSign SA 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 the *DocuSign Signature Appliance User Guide*.

Using an External CA in Automated Mode

The *CA Setup* dialog box appears during the course of DocuSign SA 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 SA can be properly verified without having to install the DocuSign SA 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 DocuSign SA from the external CA, the end user can start signing documents.

An example of scenarios in which an external CA is useful are cases where customers may wish to use signing certificates that are part of a special program such as TSCP or the Adobe

Approved Trusted List (AATL), where the certificate enrollment characteristics and parameters differ from those of the certificate provided by the internal Appliance's CA.

The following External CAs can be defined as part of the DocuSign SA installation:

- DocuSign TSCP – only when DocuSign SA is deployed in Microsoft Active Directory mode
- DocuSign CA
- Symantec
- Comodo – Not supported anymore

The following sub-sections explain how to configure each of these external CAs.

Note that the organization's policy may not allow direct communication between the DocuSign Signature Appliance and the external CA. In such cases, you can optionally configure the DocuSign Signature Appliance to communicate with the external CA through the organization's proxy server. To do so, you must configure the proxy settings defined in *Advanced Settings* as part of *Installing the DocuSign Signature Appliance Software*.

> ***Note***: In a multiple CA deployment, only the default CA can be configured to use *external CA in automated mode;* other CAs can be either regular internal CAs or subordinate CAs.

Using an External CA in Automated Mode – Comodo

This mode is not supported any more.

Using an External CA in Automated Mode – DocuSign TSCP

The *CA Setup* dialog box appears during the course of DocuSign SA software installation. It enables setting DocuSign TSCP CA in automated mode. It is allowed to use the DocuSign TSCP CA only when DocuSign SA is deployed in Microsoft Active Directory mode.

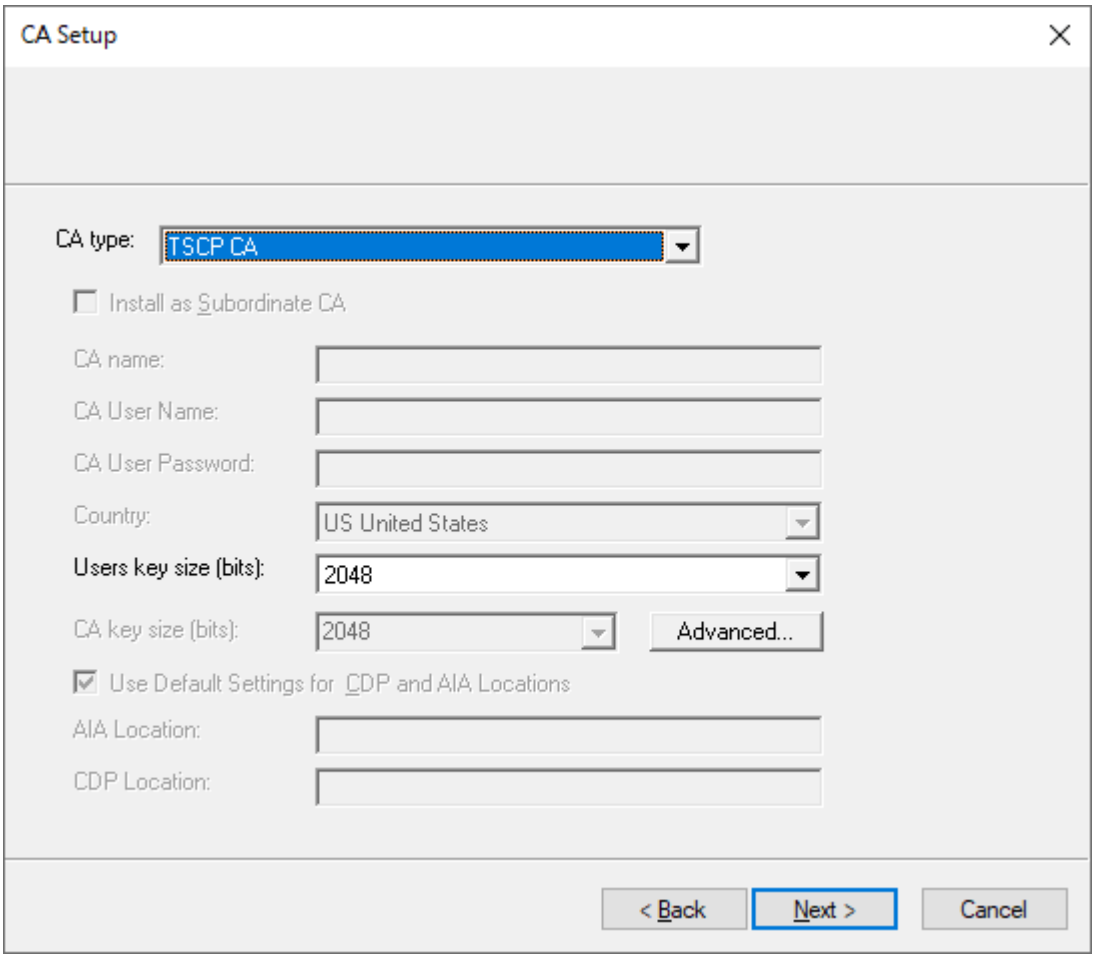


Figure 27 CA Setup – DocuSign TSCP CA Dialog Box

To specify the DocuSign TSCP CA:

1. Specify **TSCP CA** in the **CA type** field.
2. Enter the following information:
   - **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.
     The minimal user key size is 2048 bits and the maximum user key size is 4096 bits.
3. After completing CA Setup, continue with Step *12* of installing DocuSign SA in a Microsoft Active Directory Environment.

When installation is complete, an internal RA (Registration Authority) authentication key is generated inside the Appliance. The authentication key will be used to securely communicate with the DocuSign CA.
A certificate request file for this authentication key will be created. You will be requested to save the file.

4. Save the file and email it to your DocuSign technical contact for approval.

   DocuSign will reply with an authentication certificate after your organization undergoes a user identication policy review.

   At this stage final installation is ended, however, no signature keys are generated for the users, which means that no user can perform a digital signature operation until CA information upload is complete.

5. Upload CA information to DocuSign SA, as described in *Uploading CA Information to DocuSign SA in the case of DocuSign TSCP CA or DocuSign CA*.

   At the end of the process, DocuSign SA will be fully interfaced with the DocuSign TSCP CA service for the purpose of automatically managing the Appliance certificates.

Note: Deploying the DocuSign Signature Appliance to use DocuSign TSCP requires many initial and ongoing procedures handled by the organization and the organization's employees/users. One of the major requirements is an employee/user identification process handled by a trusted role. As part of the employee/user onboarding process, the employee/user will be required to sign a DocuSign envelope.
A similar envelope will need to be signed if the employee's email or his/her common name has changed.

Using an External CA in Automated Mode – DocuSign CA

The *CA Setup* dialog box appears during the course of DocuSign SA software installation. It enables setting DocuSign CA in automated mode.

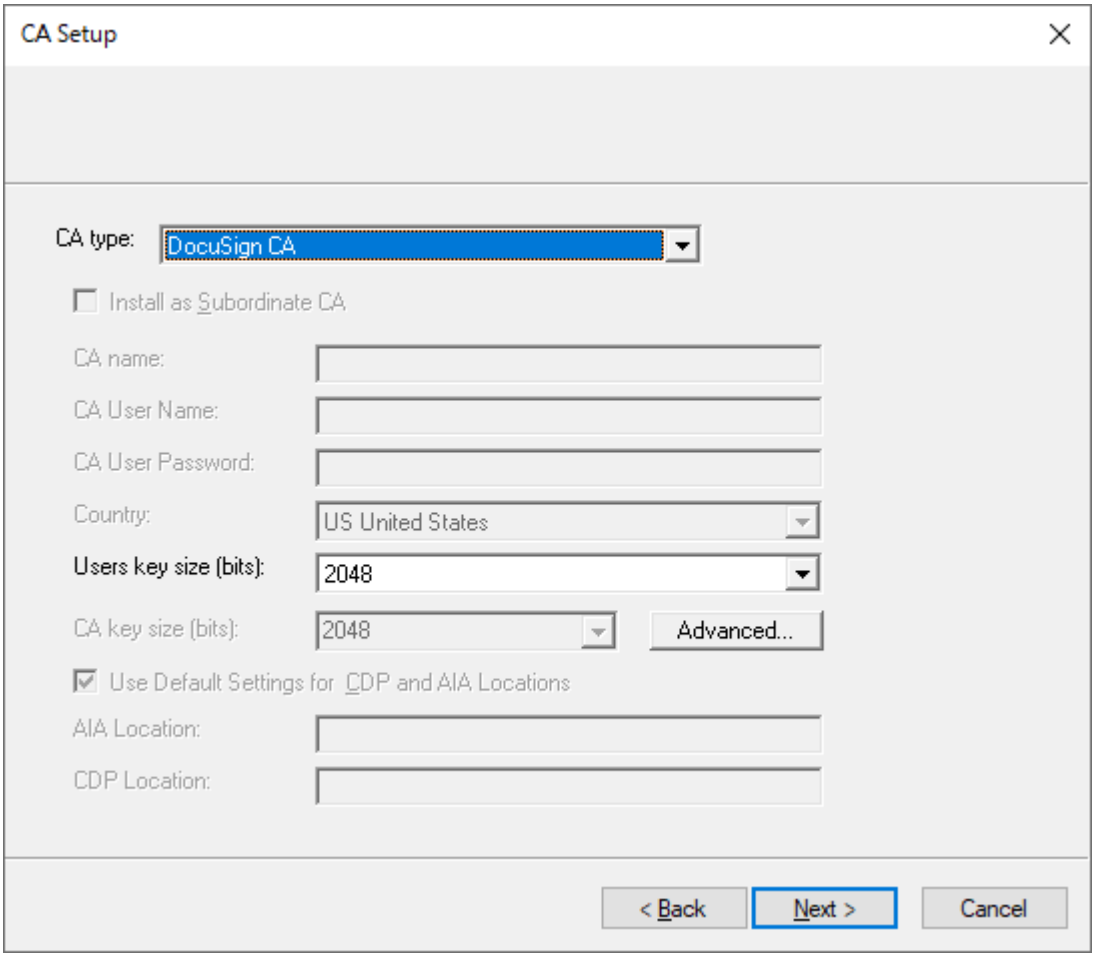


Figure 28 CA Setup – DocuSign CA Dialog Box

To specify the DocuSign CA:

1. Specify **DocuSign CA** in the **CA type** field.
2. Enter the following information:
   - **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.
     The minimal user key size is 2048 bits and the maximum user key size is 4096 bits.
3. After completing CA Setup, return to the software installation procedure as follows:
   - If you are installing DocuSign SA in a Microsoft Active Directory Environment, continue with Step *12*.

- If you are installing DocuSign SA in a Directory Independent Environment, continue with Step *8*.

When installation is complete, an internal RA (Registration Authority) authentication key is generated inside the Appliance. The authentication key will be used to securely communicate with the DocuSign CA.
A certificate request file for this authentication key will be created. You will be requested to save the file.

4. Save this file and email it to your DocuSign technical contact for approval.

   DocuSign will reply with an authentication certificate after your organization undergoes a user identication policy review.

   At this stage final installation is ended, however, no signature keys are generated for the users, which means that no user can perform a digital signature operation until CA information upload is complete.

5. Upload CA information to DocuSign SA, as described in *Uploading CA Information to DocuSign SA in the case of DocuSign TSCP CA or DocuSign CA*.

   At the end of the process, DocuSign SA will be fully interfaced with the DocuSign CA service for the purpose of automatically managing the Appliance certificates.

Uploading CA Information to DocuSign SA in the case of DocuSign TSCP CA or DocuSign CA

Upload the CA information to DocuSign SA using the DocuSign SA Administration MMC.

1. Login as the Appliance Administrator before continuing.
2. In the system tray, right-click the  icon and select **Administrative Tools → Appliances Management.**

   The *DocuSign Signature Appliance Management* window appears, showing all installed DocuSign Signature Appliances.

   Note that the current state of the default CA is *Pending CRP Upload*.

   - In the case of DocuSign TSCP CA, right-click the primary DocuSign Signature Appliance, and in the **Certificate Authorities** / **TSCP CA (Default)** select **All Tasks → Upload RA certificate reply.** The Upload CA Information window appears:
   - In the case of DocuSign CA, right-click the primary DocuSign Signature Appliance, and in the **Certificate Authorities** / **DocuSign CA (Default)** select **All Tasks → Upload RA certificate reply.** The Upload CA Information window appears:

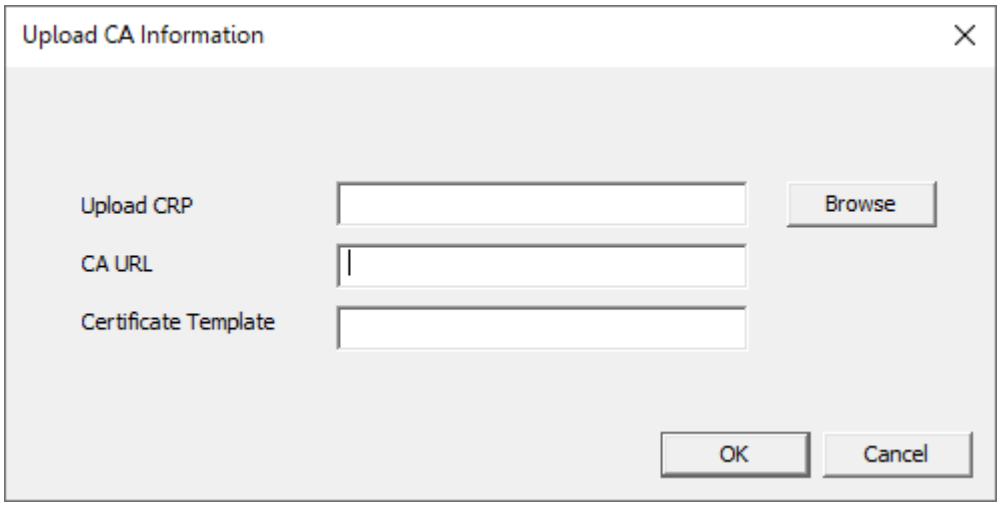
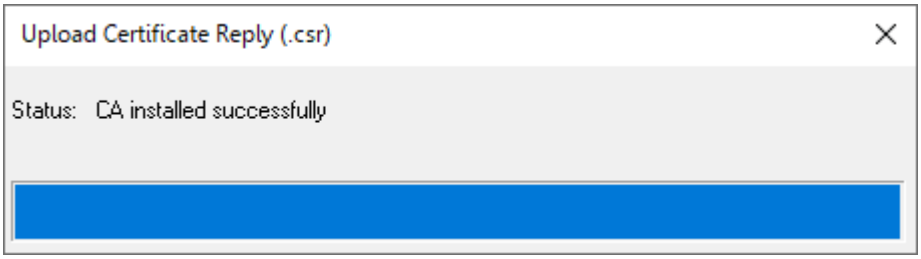


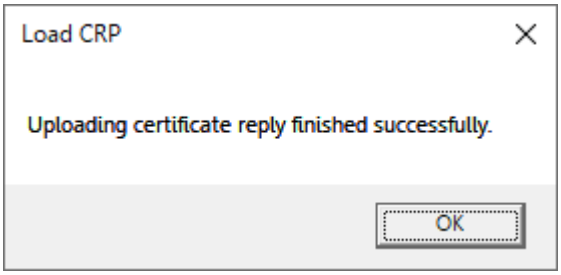
Figure 29 Upload CA Information Window

3. Enter the following information, and then click **OK**:
   - **Upload CRP** – Browse to the authentication certificate file provided by DocuSign. The default file name is *RA-certificate.pfx*.
   - **CA URL** – Enter the URL of the CA as provided to you by DocuSign.
   - **Certificate Template** – Enter the identity of the Certificate template as provided to you by DocuSign
4. Click **OK**.

   As part of the operation, the Appliance will communicate with DocuSign CA.

   Success messages will appear to indicate communication with DocuSign CA is successful.





5. Afterwards, the Appliance will make sure that each signer has a signature key and a certificate from DocuSign CA.

If the Appliance is configured to use DocuSign TSCP CA, the created certificate is compatible with the TSCP program and AATL program.

Using an External CA in Automated Mode – Symantec

The *CA Setup* dialog box appears during the course of DocuSign SA software installation. It enables setting Symantec as the External CA in automated mode.

Note: It is recommended to setup a Symantec Admin account before installing DocuSign SA with the Symantec External CA. There are several parameters defined during account setup in the Symantec Portal that are required for the DocuSign SA installation. For information on setting up an account, refer to *Creating a Symantec Profile Preparatory to Configuring Symantec as DocuSign SA's External CA*.

Note: The process of setting Symantec as the External CA involves direct interaction with Symantec (http://www.symantec.com). For more information on Symantec, refer to the Symantec website.

Note: The end user certificate and its values are handled by the Symantec CA and the relevant profile used. For example, the purpose of the signature key is defined according to the *key-usage* and the *extended-key-usage* attributes. Keep this in mind when defining these and other attributes

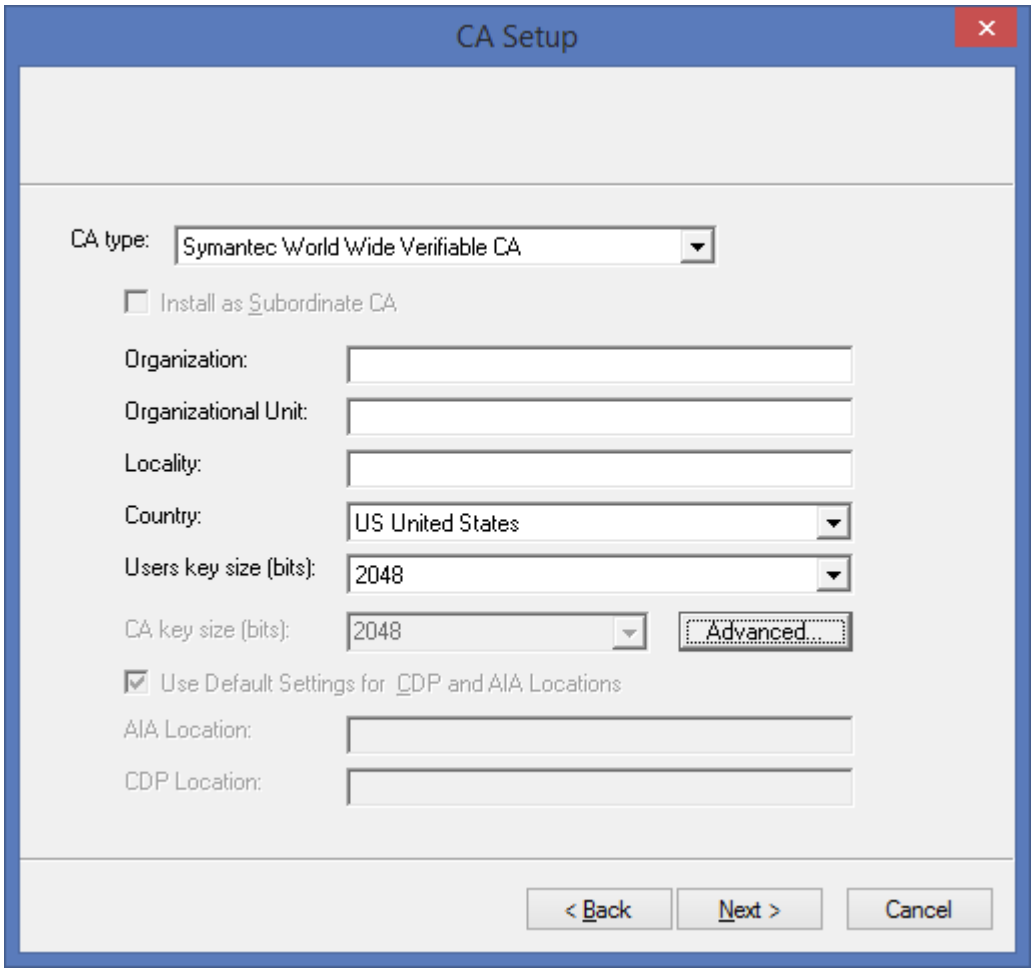


Figure 30 CA Setup – Symantec CA Dialog Box

To specify the Symantec CA:

1. Specify **Symantec World Wide Verifiable CA** in the **CA type** field.
2. Enter the following information:

   - **Organization** – The organization producing the user certificate. Depending on the deployment, the CA may decide the Organization according to its policy. This field is optional.
   - **Organizational Unit** – The requested organizational unit of the user certificate. Depending on the deployment, the CA may decide the Organizational unit according to its policy. This field is optional.

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

   - **Locality** – The requested locality of the user certificate.

- **Country** – The requested country of the user certificate. Depending on the deployment, the CA may decide the Country according to its policy.
- **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. You should use a key size of 2048 bits.

- If you are installing DocuSign SA in a Microsoft Active Directory Environment, continue with Step *12*.
- If you are installing DocuSign SA in an LDAP based Environment, continue with Step *10*.
- If you are installing DocuSign SA in a Directory Independent Environment, continue with Step *8*.

When installation is complete, the following message appears:

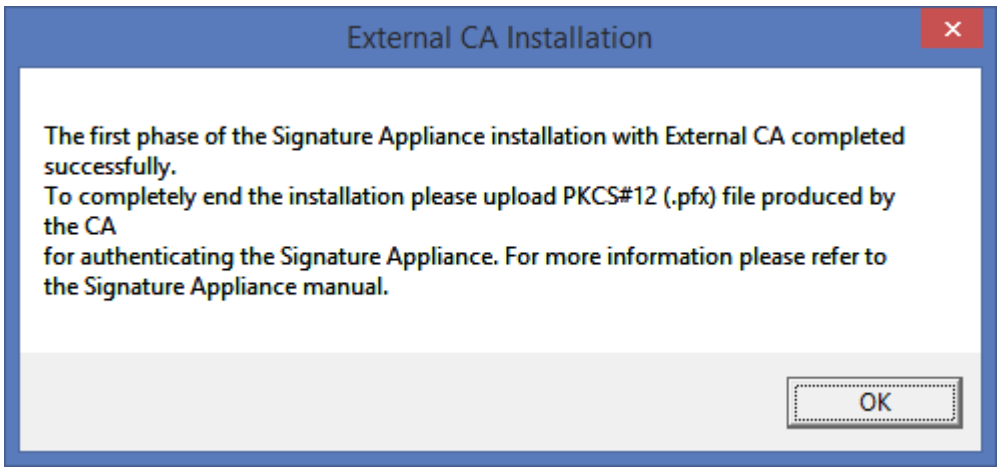


Figure 31 External CA Installation message

At this stage final installation is postponed until CA information is uploaded to the DocuSign Signature Appliance. No user information is generated, and thus no user can perform a digital signature operation until CA information upload is complete.

3. Upload CA information to DocuSign SA, as described in *Uploading CA Information to DocuSign SA in the case of Symmantec CA*.

   At the end of the process, DocuSign SA will be fully interfaced with the Symantec service for the purpose of automatically managing DocuSign SA users' certificates.

Uploading CA Information to DocuSign SA in the case of Symmantec CA

Upload the CA information to DocuSign SA using the DocuSign SA Administration MMC.

1. In the system tray, right-click the icon and select **Administrative Tools → Appliances Management.**

   The *DocuSign Signature Appliance Management* window appears, showing all installed DocuSign Signature Appliances.

   Note that the current state of the DocuSign SA installation is *Waiting for PFX from CA*.

Right-click the primary DocuSign Signature Appliance, and in the **Certificate Authorities** / **Symantec WWV CA (Default)** select **All Tasks** → **Upload .pfx** certificate. The Upload CA Information window appears:

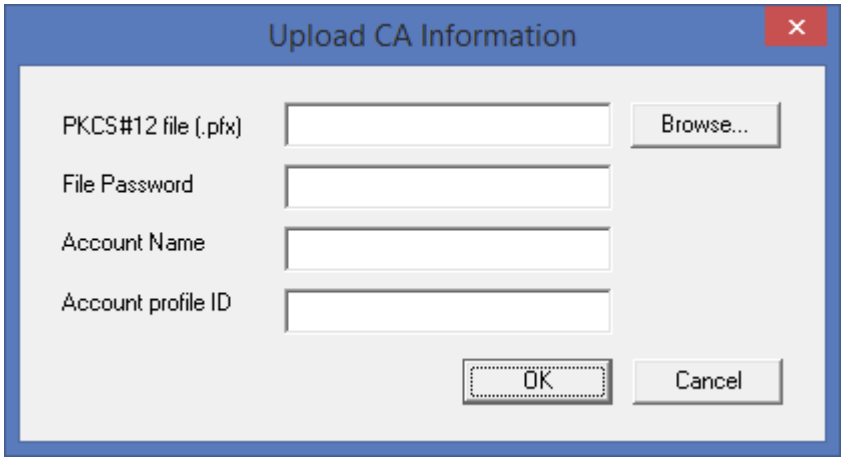


Figure 32 Upload CA Information Window

2. Enter the following information, and then click **OK**:

   - **PKCS#12 file (.pfx)** – Browse to the PKCS#12 authentication key file provided by the Symantec portal. The default file name is *RA-certificate.pfx*.
   - **File Password** – Enter the protection password provided by the Symantec portal.
   - **Account Name** – Enter your account Number in Symantec. To obtain your Account Number, click the **Settings** icon (*Figure 44*) and select the **Manage account and sub-accounts** option. In the *Manage Accounts* window that appears, note the number under the account name. This is the number to be entered to the **Account** *Name* field. In the example below, the number is *775243*.

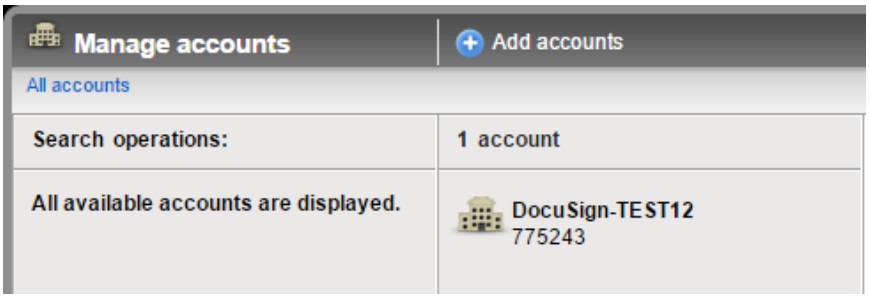


Figure 33 Manage Accounts

   - **Account Profile ID** – This information refers to the certificate profile used. To obtain the profile ID, click the **Settings** icon (*Figure 44*) and select the **Manage Certificate Profiles** option. In the *Manage certificate profiles* window that appears, select the relevant certificate profile, which is My Certs in the example below. Note the Certificate Profile OID. This is the dotted numbered string which you should enter in the **Account Profile OID** field. In the example below, the profile ID is:
     2.16.840.1.113733.1.16.1.2.5.6.1.149026865

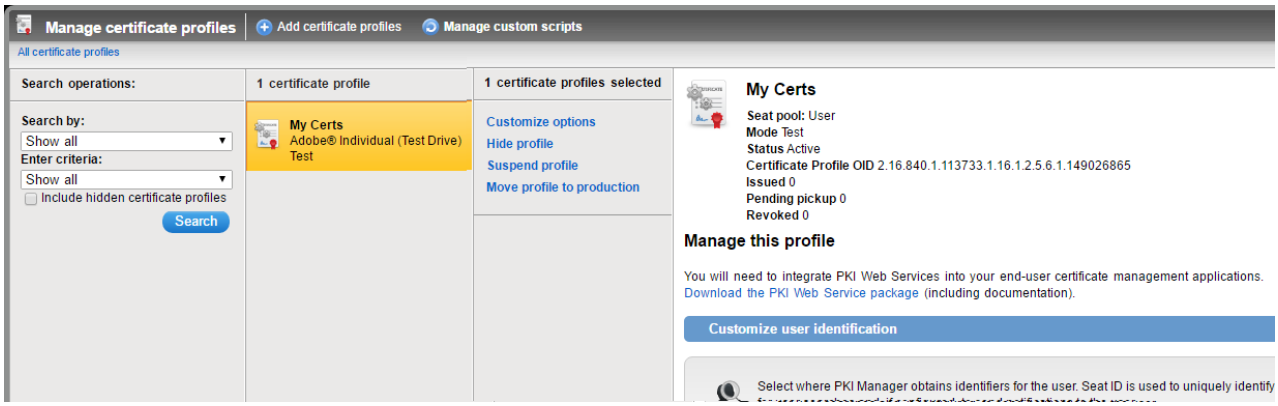


Figure 34 Manage Certificate Profiles

After you click **OK**, the authentication Private Key and certificate are uploaded to the Appliance and used as part of the communication between the DocuSign Signature Appliance the Symantec.

3. If Active Directory is used, user synchronization is performed automatically.
   This operation results in DocuSign SA generating a signature key for each user and receiving a certificate for this user from Symantec.

   In a Directory Independent environment, you must activate the `Users Management` utility to create DocuSign SA 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 SA.

> ***Note:*** It is very important to save the *Account Name*, *Account Profile ID* and any other information related to accessing the Symantec account such as the admin software key and the password to access this key. You will need these when your authentication key file expires and you need to renew it.
> For more information on how to renew your authentication key file, refer to *Renewing the DocuSign CA's RA certificate*

When using DocuSign TSCP CA or DocuSIgn CA as the automatic external CA, the DocuSign Signature Appliance is authenticated to the DocuSign CA service using an authentication key and an authentication certificate. When the authentication certificate expires, it is required to regenerate the authentication key and get a new certificate. This process occurs every three years.

To renew the DocuSign CA's RA authentication key and certificate:

1. In the DocuSign Signature Appliance Management window (Figure 57), right-click the relevant DocuSign Signature Appliance and select the default CA **in the Certificate** Authorities section. Then **select all Tasks → Download RA certificate request.**

   A new DocuSign CA's RA certificate request is downloaded.

2. Send the certificate request to DocuSign.

DocuSign will reply with a new certificate.

3. In the DocuSign Signature Appliance Management window (Figure 57), right-click the relevant DocuSign Signature Appliance and select the default CA **in the Certificate** Authorities section. Then **select all Tasks → Upload RA certificate reply.**

   The Upload CA Information window appears:

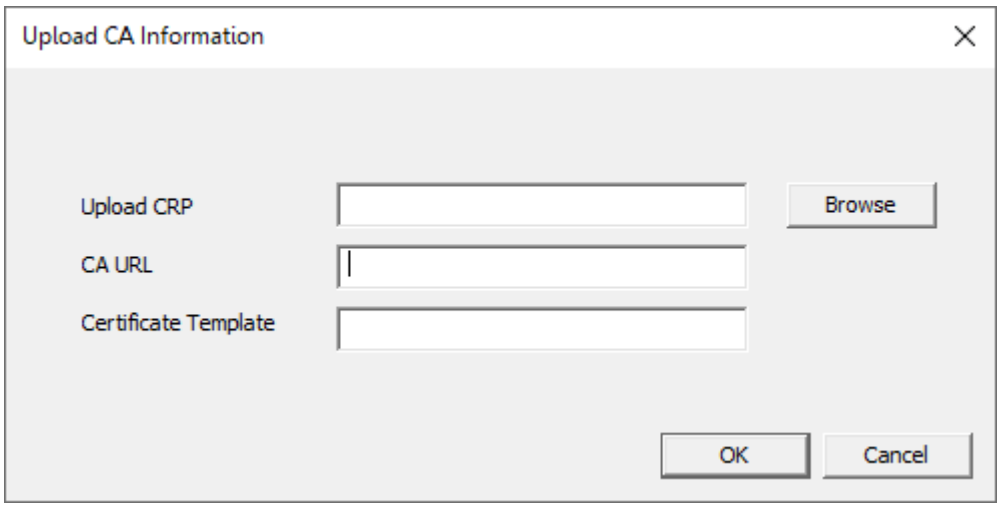


Figure 57 Upload CA Information Window

4. Enter the following information, and then click **OK**:
   - **Upload CRP** – Browse to the authentication certificate file provided by the DocuSign. The default file name is *RA-certificate.pfx*.
   - **CA URL** – Enter the URL of the CA as provided to you by DocuSign.
   - **Certificate Template** – Enter the the identity of the Certificate template as provided to you by DocuSign.
5. Click **OK**.

   As part of the operation, the Appliance will communicate with DocuSign CA.

   A success message appears, indicating that communication with DocuSign CA is successful.

Renewing the Symantec Authentication Key File

Verifying end-users can use the Symantec CA

In order to get properly generated certificates from Symantec CA, the following needs to be taken care of for every user that is supposed to get a certificate:

- The user should have an email address either in his/her Active Directory/LDAP account or in his/her DocuSign SA account. If there is an empty email address for the user, a certificate will not be issued for this user.
- The user should have a first name and last name in his/her Active Directory/LDAP account or in his/her DocuSign SA account. If one of these attributes are missing, a certificate will not be issued for this user.

Note: The Appliance administrator can view all users that failed to receive a certificate from the Symantec CA service, by viewing the DocuSign SA log file.

Creating a Symantec Profile Preparatory to Configuring Symantec as DocuSign SA's External CA

If you are planning on using DocuSign SA with the Symantec External CA, it is recommended to setup a Symantec Admin account before installing DocuSign SA. There are several parameters you define during account setup in the Symantec Portal that are required for the DocuSign SA installation.

Configure the following in Symantec before installing DocuSign SA:

1. *Creating a New Account for the Organization in Symantec*
2. *Creating a profile in Symantec*
3. *Defining a Software based Key*
4. *Uploading the Certificate Request File to the Symantec Portal*

Creating a New Account for the Organization in Symantec

To create a new account for the organization in Symantec:

Note: If you wish to open a Production account, contact Symantec for more information on how to initiate opening a production account.

1. Go to https://www.symantec.com/theme/free-trial-mpki and fill in the registration information.
2. After submission you will receive an activation email. Click the activation link to start the process of installing the Symantec PKI Client and an administrator certificate. The Symantec PKI Client will enable you to access the Symantec portal and acts as a browser extension.

   The following message appears after pressing the activation link:

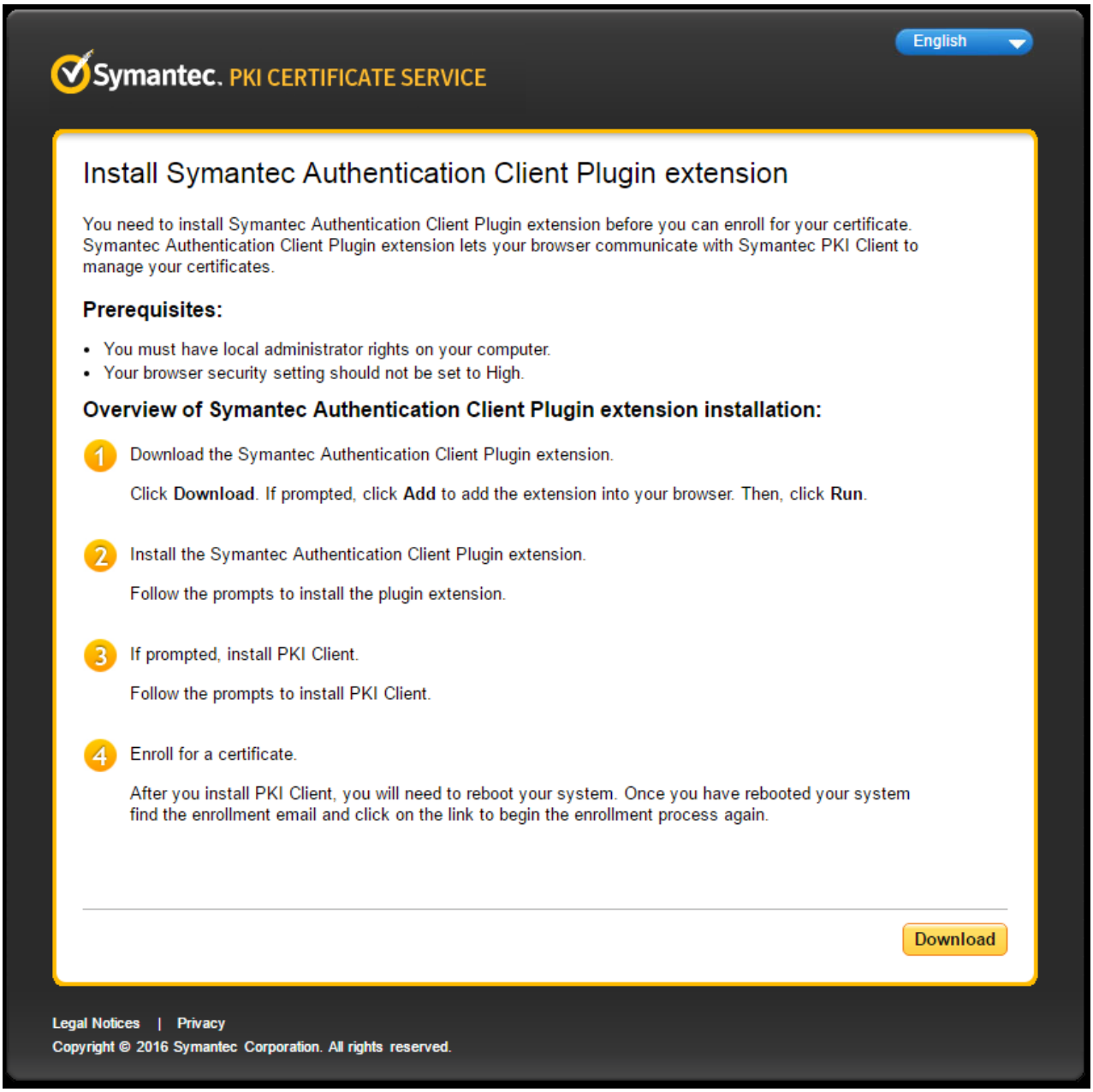


Figure 35 Install Symantec PKI Client Plugin Extension

3. Download and install the Symantec PKI Client software (if not installed already). This is a standard installation that ends with the following window and a restart:

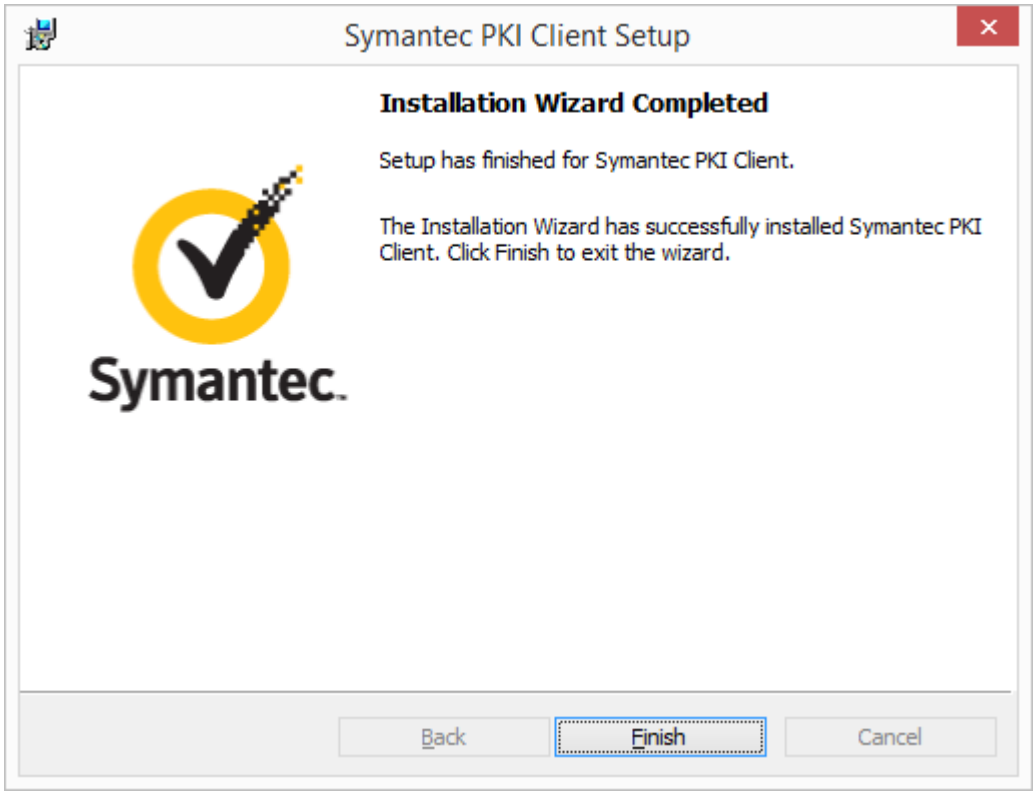


Figure 36 Symantec PKI Client Setup – Installation Complete

4. After the Symantec PKI client is installed, continue and install the administrator certificate by clicking **Install Certificate** in the window below:

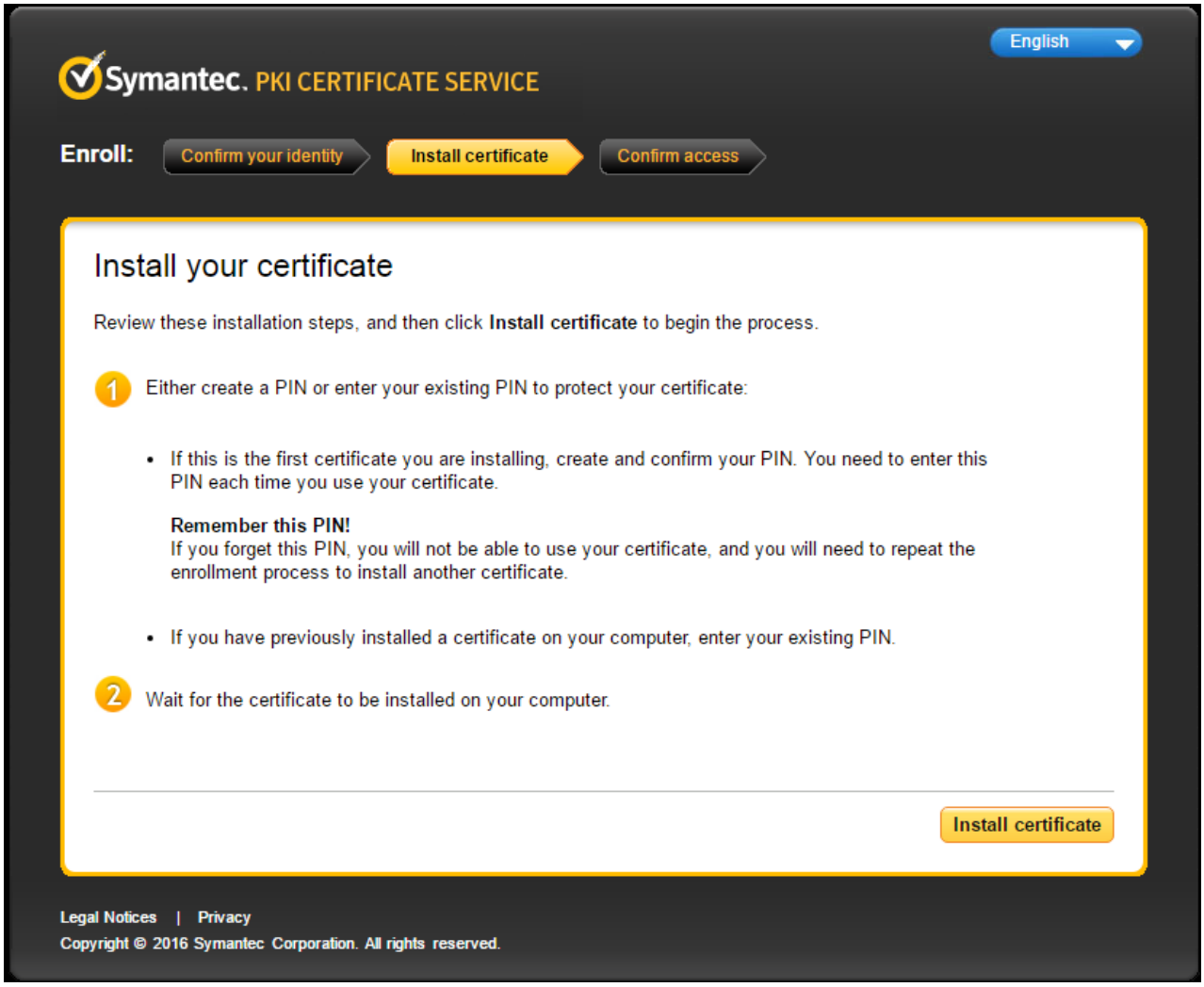


Figure 37 Selecting to install a Symantec PKI certificate

5. In the following *Create your new PIN* window that appears, enter the Pin Code that will enable you to access a locally generated software key and thus access the Symantec portal as an administrator and configure your account.



Figure 38 Create your new PIN - Symantec PKI

6. When you are prompted with the following message, you can logon as an administrator to the trial system:

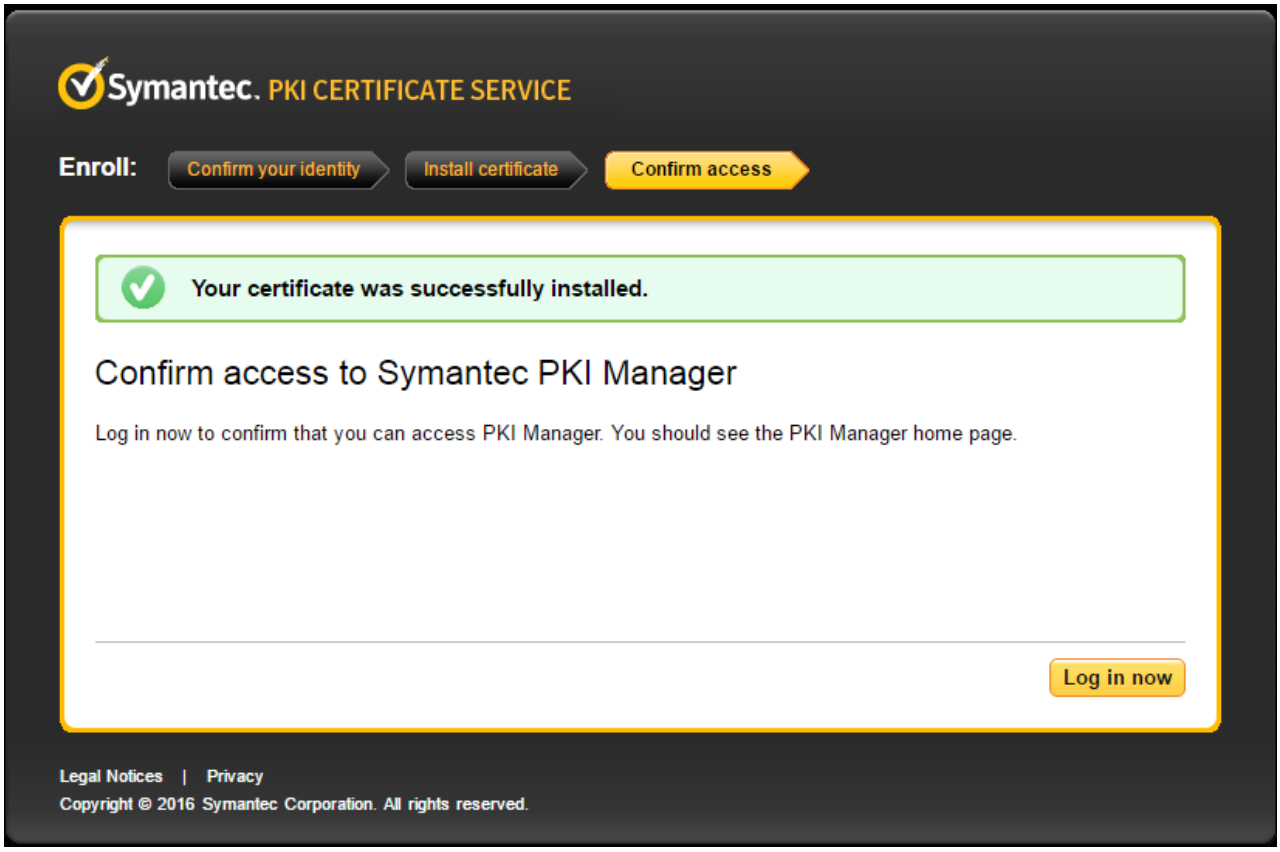


Figure 39 Confirm Access - Symantec PKI

> ***Note:*** There is a difference between this administrative account that enables you to connect to the Symantec portal for the purpose of configuration and watching status information, and the administrative account that will be used by the DocuSign Signature Appliance to access the Symantec portal as a Registration Authority (RA) for generating certificates for users that have signature keys inside the DocuSign Signature Appliance.

7. Each DocuSign SA user certificate is associated with a Symantec certificate template, which is defined as a Certificate Profile entity in the Symantec CA service.
   Connect to your Symantec account by clicking **Log in now** (Figure 39) and create a new Certificate Profile as described in *Creating a profile in Symantec*.

Creating a profile in Symantec



Figure 40 Selecting Manage Certificate Profiles

1. Log into Symantec.
2. Click the **Manage Certificate Profile** icon and then use the **Add Certificate Profile** option.
3. In the *Select mode* screen, select the **Test Mode** option.
4. In the *Select template* screen, select the type of certificates to use. In test mode, please select *Adobe Individual (Test Drive)*.

> ***Note:*** Consult with DocuSign which certificate type to use if you require a different certificate type.

5. In the Customize options screen:
   a. Enter **Certificate Friendly Name** for the certificate profile.
   b. Set the **Enrollment method** to **PKI Web Services** and click **OK**.

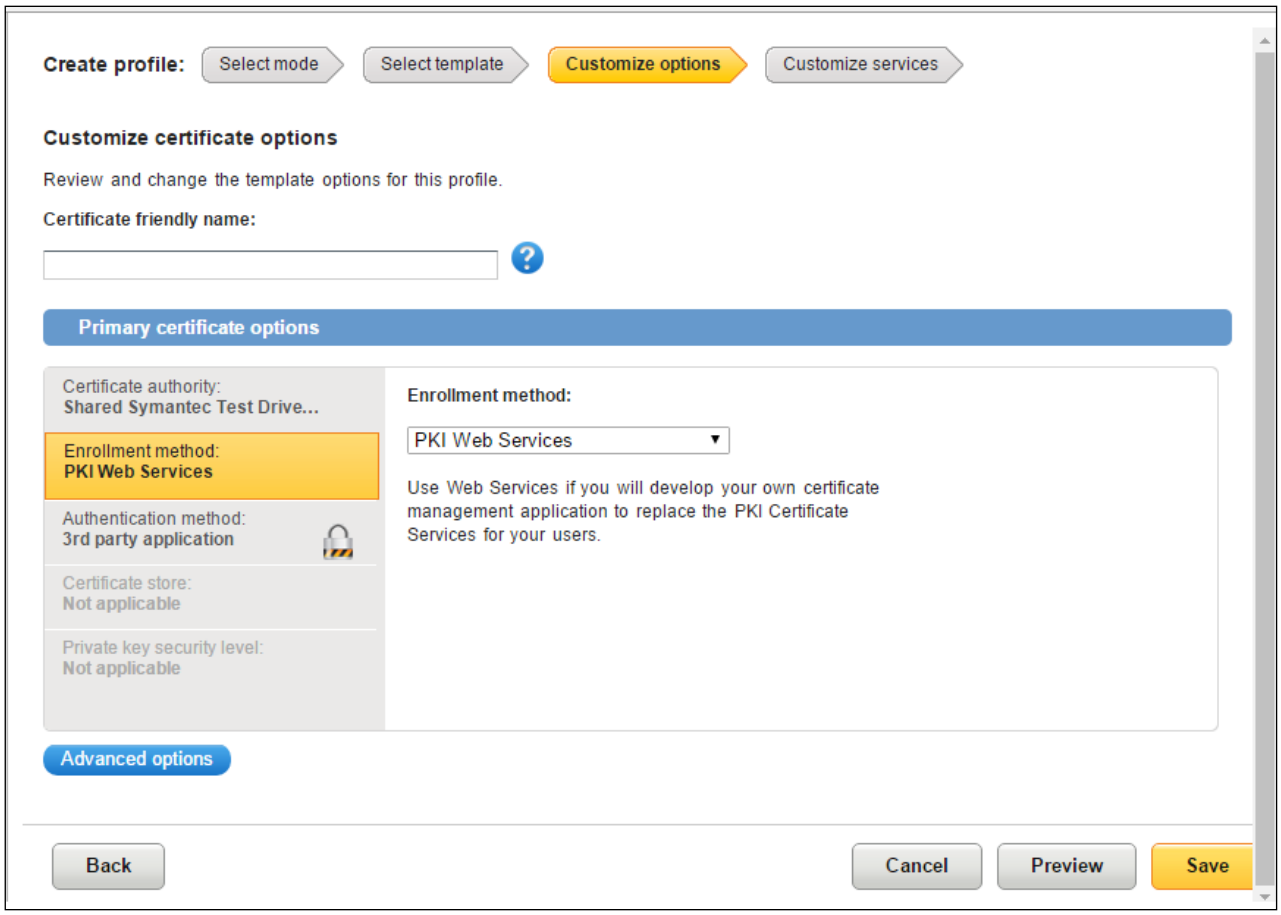


Figure 41 Creating a Symantec Profile – Customize options

6. Click **Advanced options**. The **Certificate Fields** section appears. Modify the fields so you get the following list. Basically the **Locality** field should be added and the **Organizational Unit** fields should be removed and added:

   - **Common Name** – Required and included in Webservice Request
   - **Email** – Required and included in Webservice Request
   - **Country** – Required and included in Webservice Request
   - **Organization** – Is a fixed value and determined by the account name
   - **Locality** – Required and included in Webservice Request
   - **Organizational unit** – this item should be removed and inserted again with **Required – Yes** and included in **Source for the field's value** - **Webservice Request**.

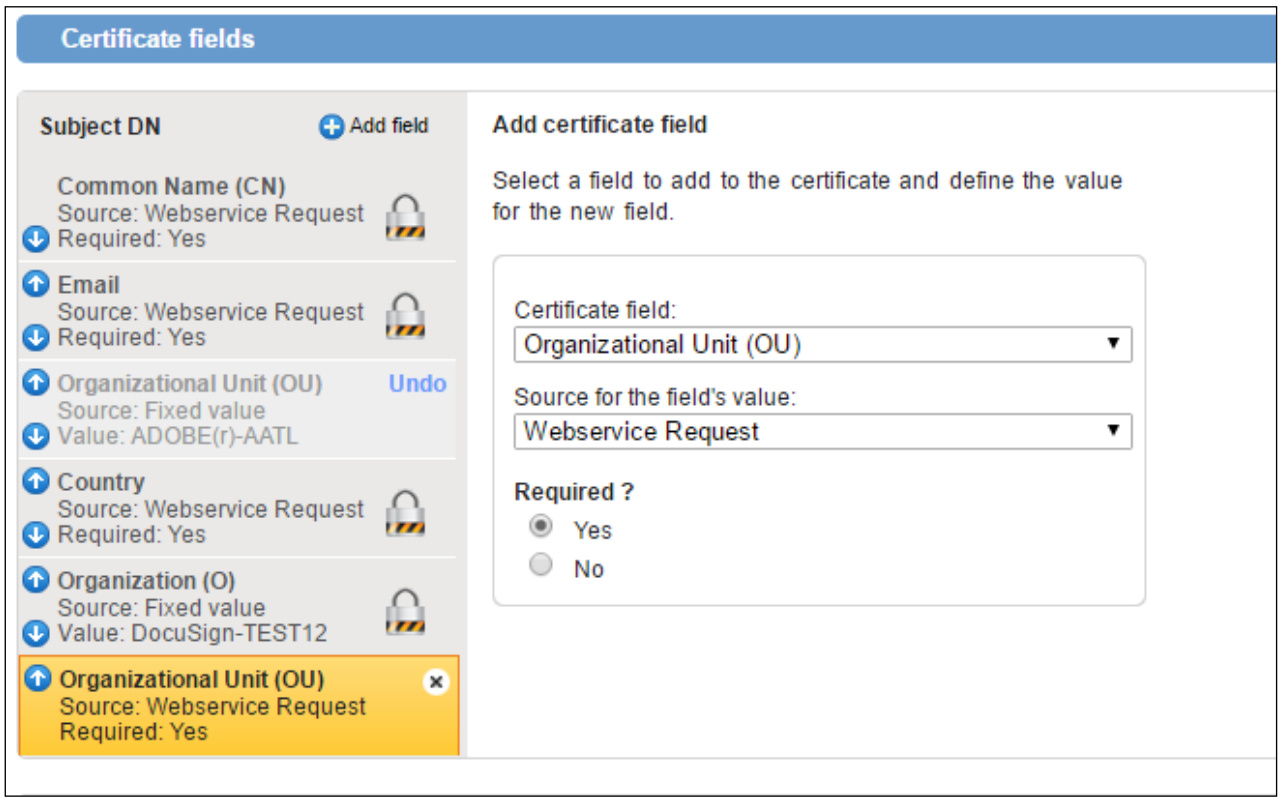


Figure 42 Certificate Fields

7. Add the following additional extensions:
   - Adobe CDS Custom Extension for Time Stamp
   - Adobe CDS Custom Extension for OCSP Revocation.
8. Go to **Additional Extensions** and mark these extensions as True. They are marked as False by default.
9. In the **additional certificate** option make sure the key size is 2048 bits

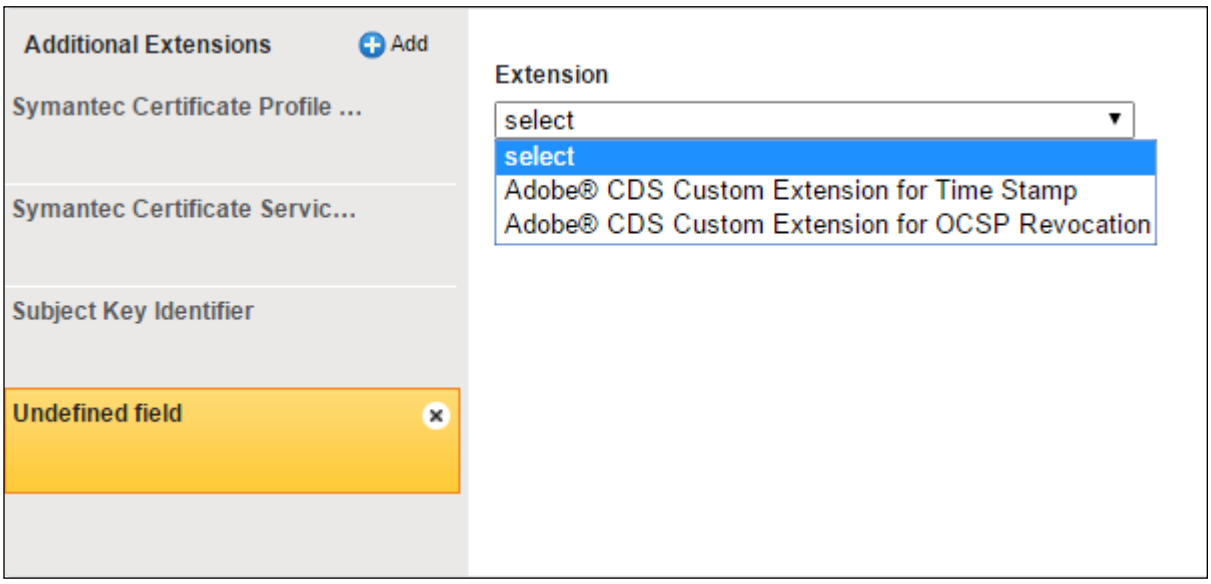


Figure 43 Additional Extensions

10. Save the Certificate Profile.

Defining a Software based Key

DocuSign SA interacts with Symantec using a client authentication scheme based on a software token. To define the software based key, open a Command Prompt window and use the special DocuSign SA tool that is based on the OpenSSL library to generate the software key and its matching authentication certificate, as follows:

1. Get the *PFXCreation.zip* package and extract it to a certain directory in your PC (for example, c:\tmp\pfx).
2. Open a Command Line application, such as cmd.exe, and go to the above directory.
3. Run the *Set.bat* command
4. Run the *CertRequest.bat* command. Keep in mind:
   a. Before running the command, call the following command *set RANDFILE=.rnd*
   b. While running the command, you will be asked to provide some application related information:
      - Enter a valid two letter code for your country name.
      - In the Common Name field, enter your Symantec account name.
      - In the Email Address field, enter your email address as configured in your Symantec account.
      - The challenge password can be left blank

An RSA key will be generated and afterwards a certificate request file will be created. The output file *CSR.csr* is the certificate request file. This file should be uploaded to the Symantec portal, as described in *Uploading the Certificate Request File to the Symantec Portal*.

Uploading the Certificate Request File to the Symantec Portal

1. In the PKI Manager Console, click the **Settings** icon and select the **Get an RA Certificate** option.

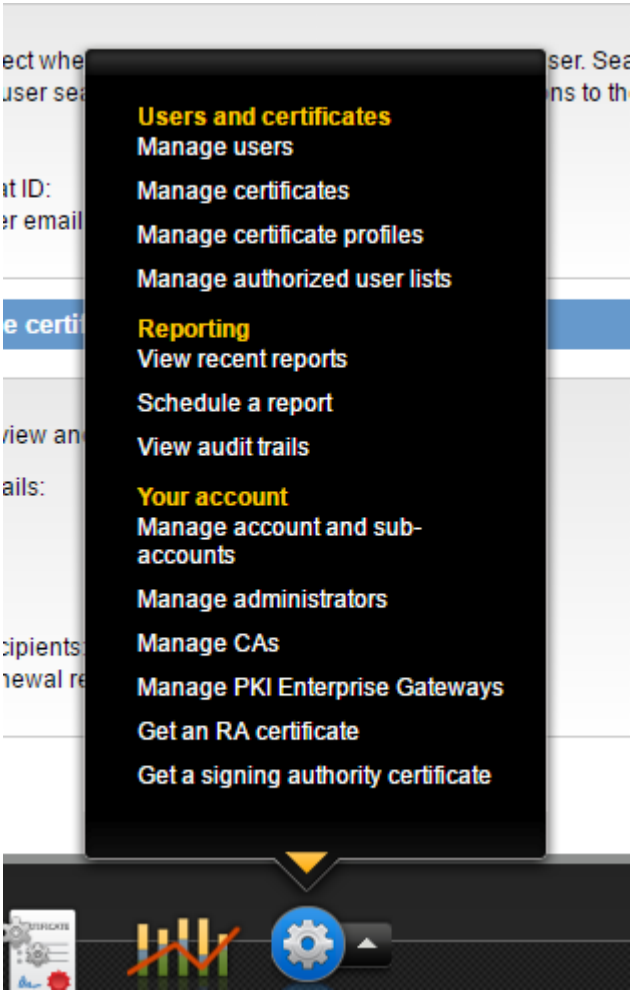


Figure 44 Symantec Settings Options

2. In the Get an RA Certificate page that appears, paste the contents of the CSR.csr file (created in *Defining a Software based Key*) into the **Paste your CSR** field.

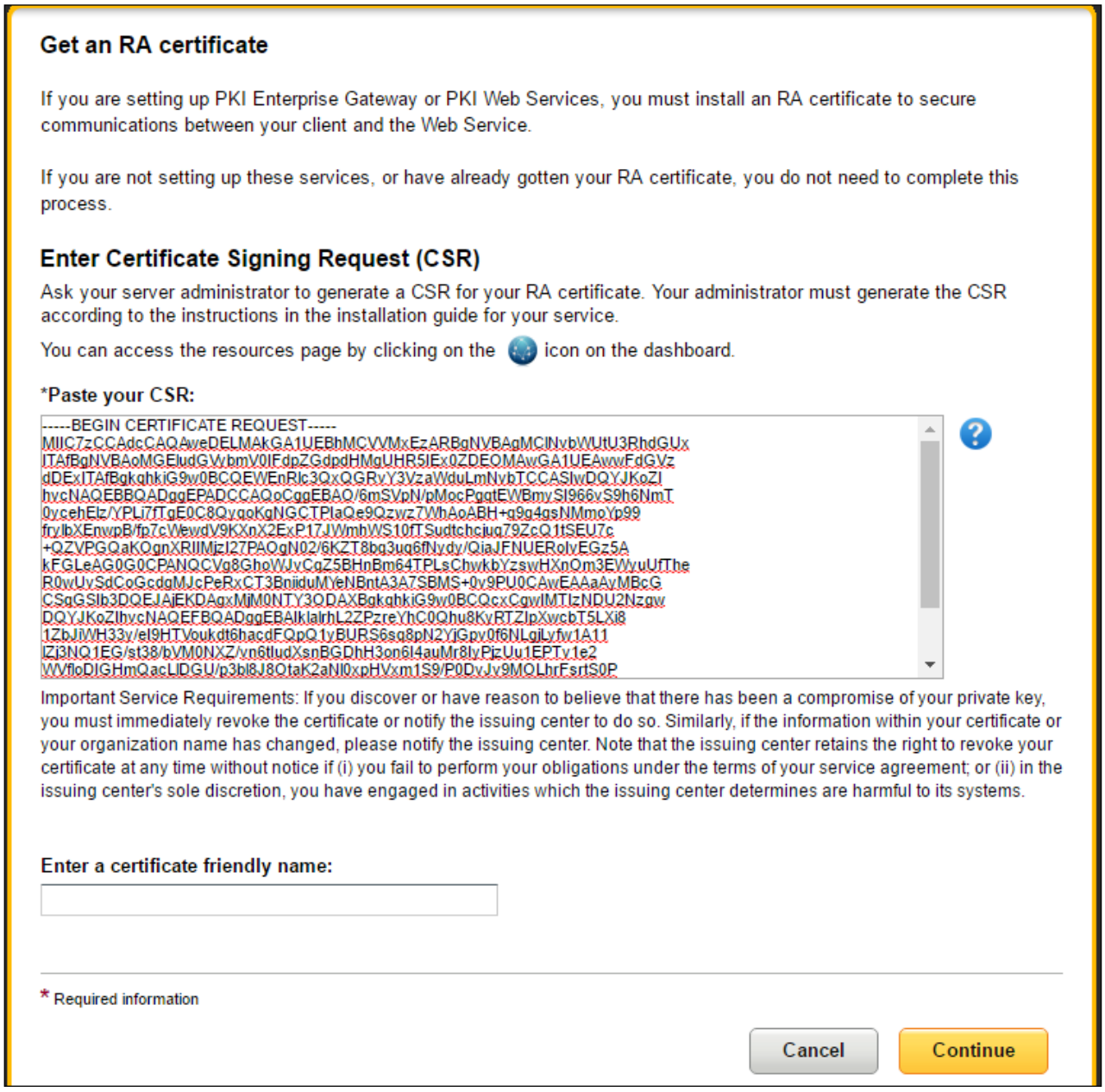


Figure 45 Get an RA Certificate Page

3. When the *Your CA certificate is ready* window appears, click **Download** to download the authentication certificate.

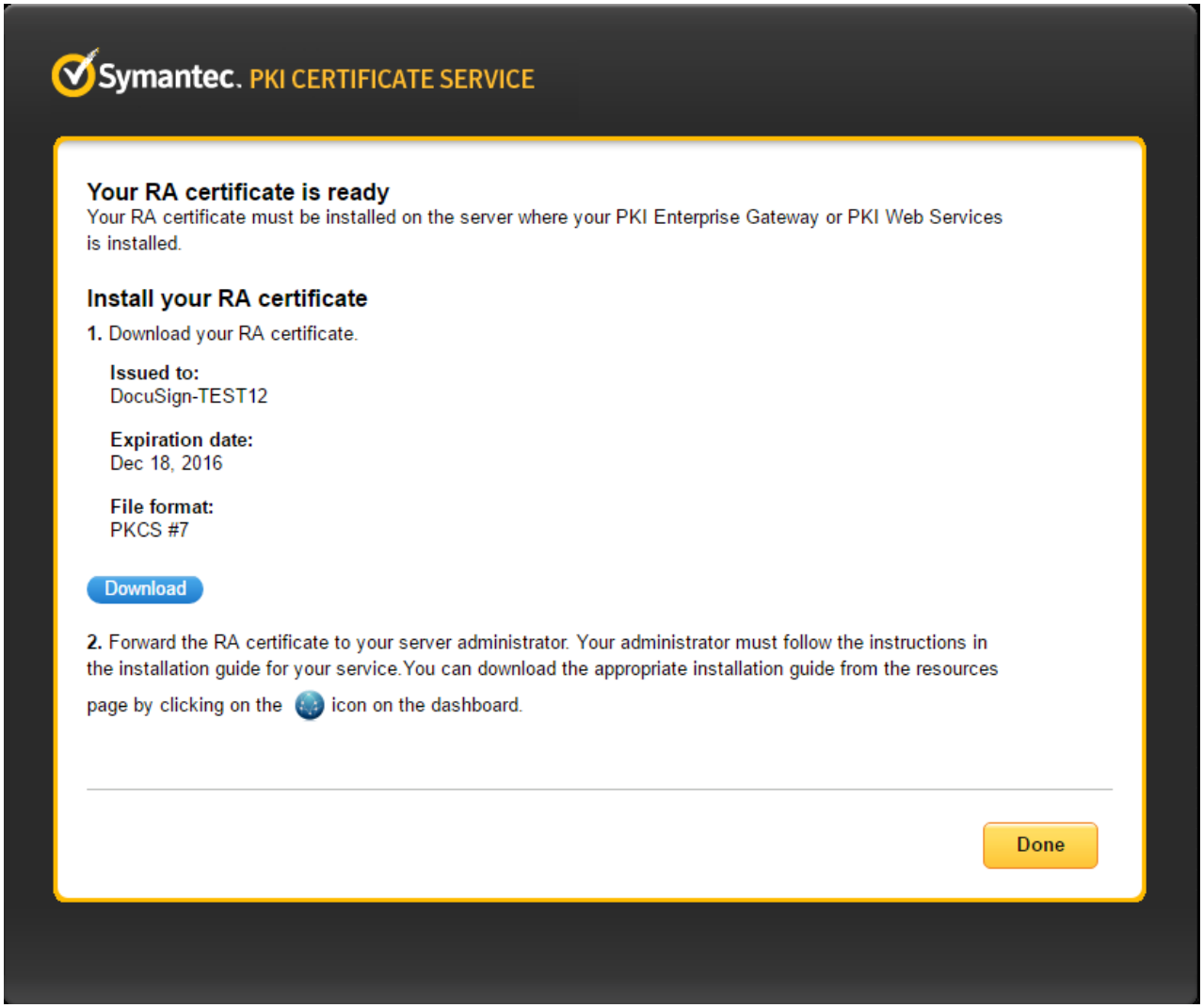


Figure 46 Your RA certificate is ready

4. Place the file named RA-Certificate.p7b in the directory in which you placed the PFXCreation.zip package (refer to *Defining a Software based Key*), and run the command cert_import.bat. You will be requested to provide a password that protects the pkcs#12 based file format that encapsulates the Software Key and the authentication certificate. Remember the provided password. It will be used when uploading the pkcs#12 key to DocuSign SA.

The file *RA-certificate.pfx* now contains the authentication key and certificate file that will be uploaded to DocuSign SA and used for accessing the Symantec Service from the DocuSign Signature Appliance.

Note: You can continue using this administrative portal to view the status of all certificates that are linked to this account. However, you should not perform any direct action on these certificates or modify any of the account parameters, since this can cause the service to become non-operational.
Instead, user certificates should be managed by the DocuSign SA through the DocuSign SA's interface to the Symantec service.

Installing DocuSign SA 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 SA installation is complete:

1. 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 DocuSign SA CA, and then created a certificate request based on the generated key. DocuSign SA then exported the CRQ that should be sent to the ROOT CA.

2. Specify the name of the CRQ file.

   The *Subordinate CA Installation* dialog box appears:

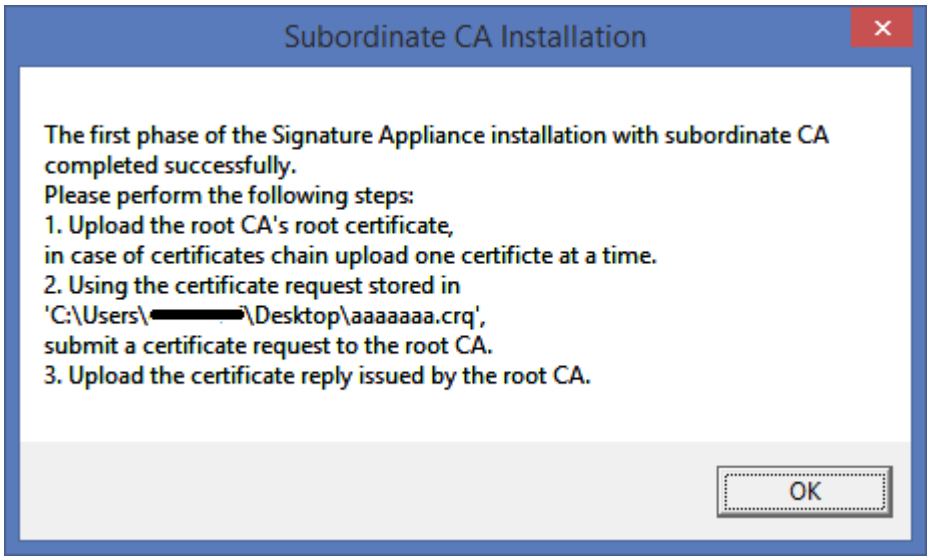


Figure 47 Subordinate CA Installation Dialog Box

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

3. Exit the DocuSign SA Administration MMC.

4. 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 DocuSign SA subordinate CA certificate. The DocuSign SA 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 SA, the complete chain of CA certificates includes only the ROOT CA certificate.

   > ***Note**:* Make sure that the certificate reply contains only the DocuSign SA 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 SA 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.

5. Once you receive the files from the ROOT CA, in the system tray, right-click the  icon and select **Administrative Tools → Appliances Management**. The *DocuSign Signature Appliance Management* window appears.
6. Login as an Appliance administrator using either the built-in administrative account or the relevant directory admin account.
7. For each file in the chain of CA certificates, perform the following:
   - Right-click the relevant **DocuSign Signature Appliance** and select **All Tasks → Upload Certificates → Upload ROOT Certificate Chain.**

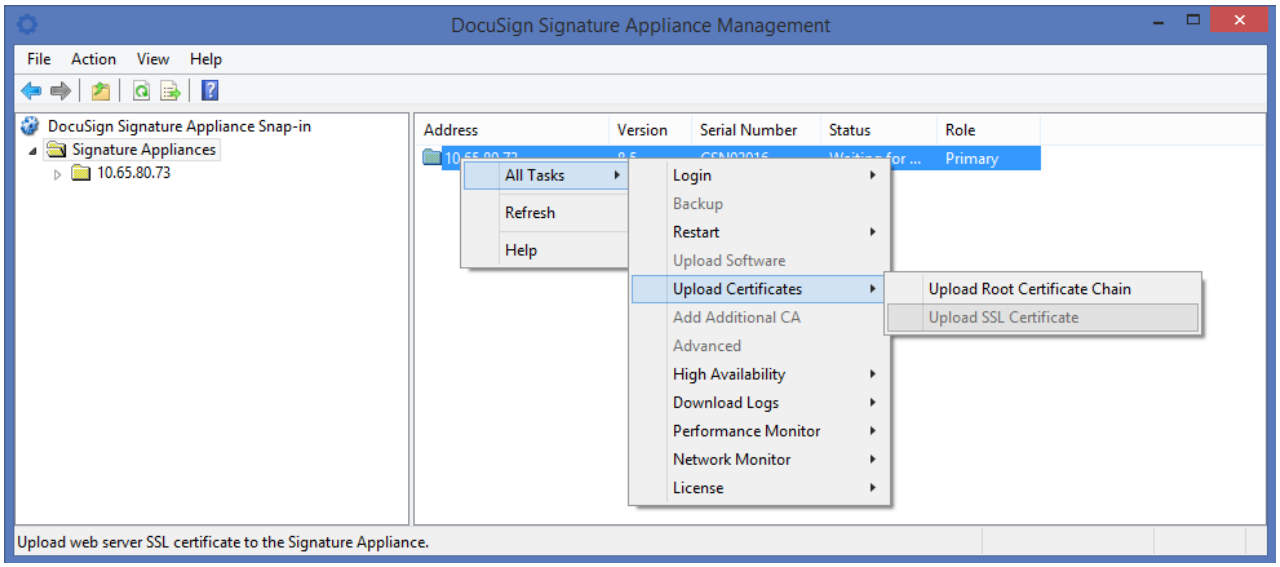


Figure 48 Subordinate CA Installation – Loading the CA Certificates

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.**

8. Right-click **DocuSign Signature Appliances** and select the relevant appliance, select **Certificate Authorities**, right-click the default certificate authority, and select **All Tasks → Upload Certificate Reply**.

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

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

A message appears: **Waiting for the CA service to restart…** and soon after DocuSign SA proceeds with the installation process. In an Active Directory, DocuSign SA now automatically creates DocuSign SA users and generates keys and certificates for them. In a Directory Independent environment, you must activate the `Users Management` utility to create DocuSign SA 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 SA.

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

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

Note: Keep in mind that setting up DocuSign SA 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 SA 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 SA release notes.

Chapter 4: Deploying the DocuSign SA Client

This chapter describes how to:

- Deploy the DocuSign SA Client, in a Microsoft-Active Directory environment, LDAP based environment, or a Directory Independent environment.
- Use the right-click menu options of the DocuSign SA Client system tray icon .
- Install the ROOT certificate to validate DocuSign SA signatures in an organization without DocuSign SA.

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

The DocuSign SA 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
- Windows Server 2016

Deployment Options

The DocuSign SA 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 SA 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 SA 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 SA client.

On a Web Server or Application Server

You can deploy the DocuSign SA client on a Web server. This enables multiple end-users to use DocuSign SA 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.

DocuSign provides digital signature APIs through a C#, C/C++ interface or COM interface. These Signature APIs are explained in detail in the *DocuSign SA 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 SA's SAPI C# or SAPI COM interface, the Web server creates a signature using DocuSign SA 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 SA through a RESTful or SOAP based Web Services interface, which is executed in the DocuSign Signature Appliance. For more information, refer to the *DocuSign SA Signature APIs Developer's Guide*.

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

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

Installing the DocuSign SA Client

The DocuSign SA Client can either be installed directly from the DocuSign Signature Appliance 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 SA client.

Note: If the DocuSign SA 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 SA client is installed. Refer to the section *Installing the Root Certificate* in the *DocuSign SA User Guide*.

DocuSign SA Client Components

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

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

The components include:

- `DocuSign Signature Appliance Client` – The standard DocuSign SA client installation without any plug-ins. The installation includes the following `.msi` files:
  - `DocuSign 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 SA without any integration efforts.
    For more information about CryptoKit, refer to the 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 CoSign Client.msi` – Provides the basic functionality for interfacing with the DocuSign Signature Appliance.
    The installation file name for 64 bit name is `ARX CoSign Client64.msi`.
  - `ARX Signature API.msi` – Provides signature APIs for enabling OEMs to use DocuSign SA with a minimal development effort.
    The APIs also include a COM-based interface that enables applications to use DocuSign SA.
    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 Signature APIs Developer's Guide*.
- `DocuSign Signature Appliance admin` – Enables administrators to install and manage DocuSign SA. The installation and management activities are described in *Chapter 3: Installing DocuSign SA* and *Chapter 6: Using the DocuSign SA Console.*
  The `DocuSign Signature Appliance admin` component is based on the following `.msi` files:
  - `ARX CoSign Admin Client.msi` – Includes all the administrative components of DocuSign SA. For example, it includes the DocuSign SA 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 in the *DocuSign SA User Guide*.
- `Microsoft Office (Word, Excel)` – The following plug-in is supported:
  - `DocuSign SA Signature Line Provider` – A digital signature plug-in for Office 2010/2013/2016 for the `.docx` and `.xlsx` file types.

  For more information, refer to Signing Microsoft Office Documents in the *DocuSign SA User Guide*.

- `DocuSign SA Prepare and Sign` – A plug-in for signing any printable data from any application. For more information, refer to *Prepare & Sign – Signing PDF and non-PDF Files* in the *DocuSign SA Client User Guide*.

Installation Pre-requisites

- To perform signatures using Office 2010/2013/2016 upon `.docx` or `.xlsx` files, it is mandatory to install .NET Framework version 4 on the client machine. .NET Framework version 4 is normally installed by default in Windows machines.

Installing the Client Directly from the CD

To install the DocuSign SA client directly from the CD:

1. Activate the *DSA Setup64.exe* installation program.

   The Choose Setup Language window appears.

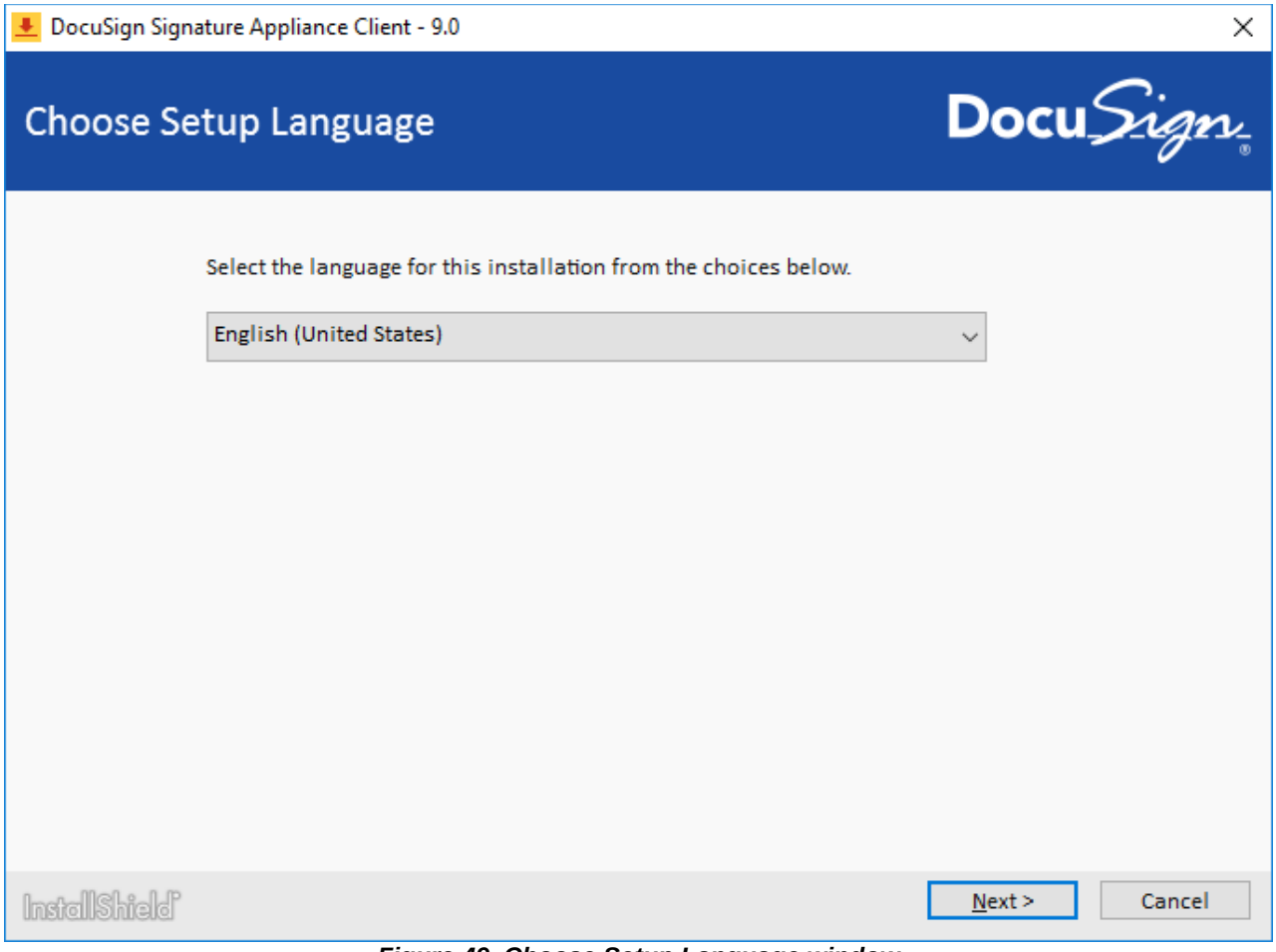


Figure 49 Choose Setup Language window

2. Choose your preferred language from the list.

   The language selection will affect the installation screens, and all end-user Client GUI elements such as Prepare & Sign, etc. It will not affect the Configuration Utility or any administrative tools.

   Click **Next.** The Setup screen appears.

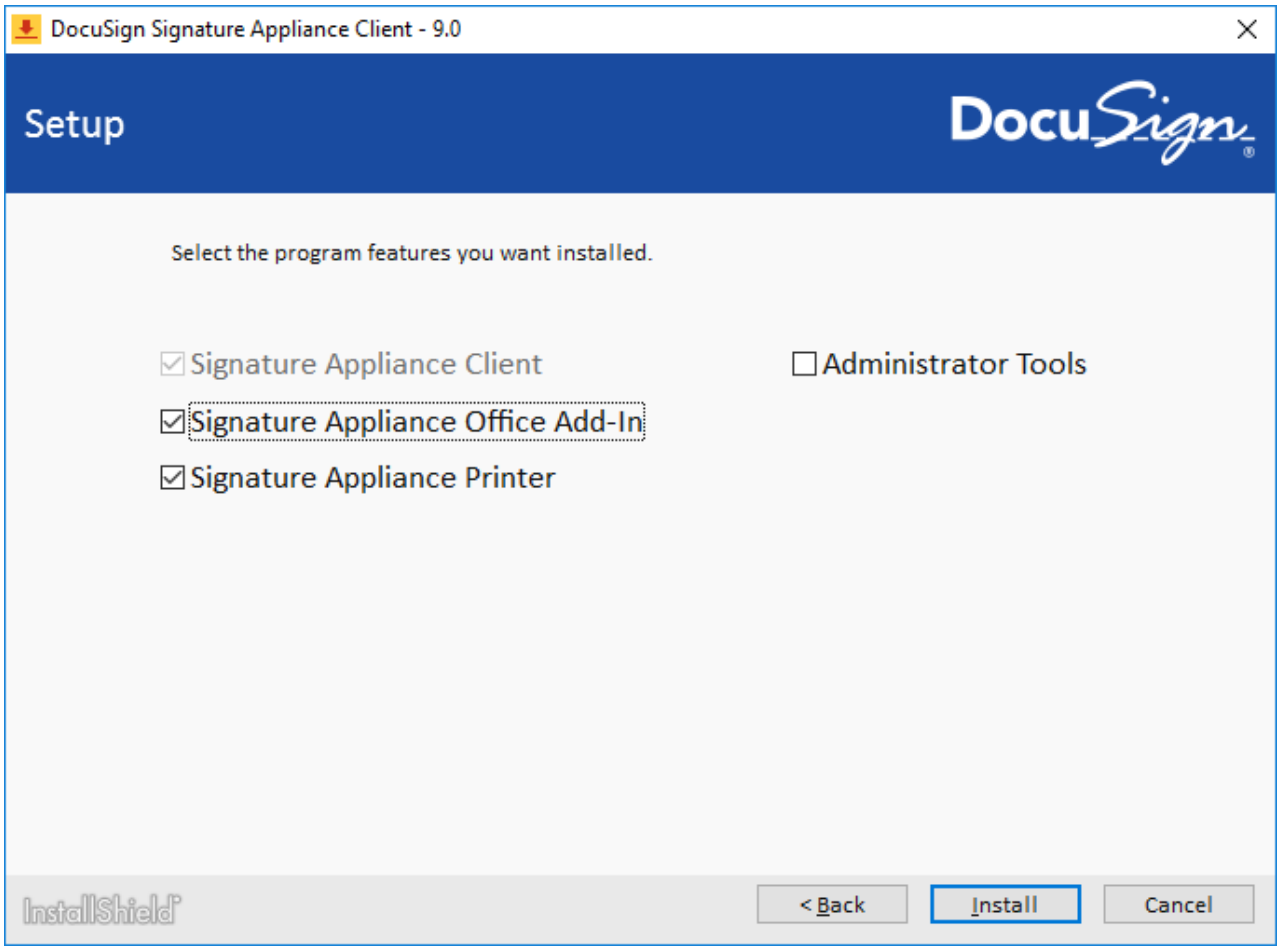


Figure 50 Select the Program Features You Want Installed

3. Select the components you wish to install, based on the designation of the current workstation. Keep in mind the following:

   - The **DocuSign Signature Appliance Client** component is always selected.
   - If the workstation is an administrative workstation, select the **Signature Appliance Admin** component.
   - If the workstation is a user workstation, select the applicable components: **Microsoft Office**, or **DocuSign SA Printer**.

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

> ***Note:*** The DocuSign SA Printer component installs a new virtual printer in the end-user's machine.

4. Click **Install**. A progress bar appears, indicating the installation status of the various DocuSign SA Client components.
5. When installation is complete, a success message appears. Click **Finish.**

Automatically Deploying the Client

Refer to *Appendix* B: Centralized DocuSign SA Client Installation for information on how to automatically deploy the DocuSign SA Client on various end user platforms.

Uninstalling the DocuSign SA Client

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

Uninstalling the DocuSign SA Client locally:

1. Go to the system Control Panel and activate the **Uninstall a Program** option.
2. Uninstall the **DocuSign Signature Appliance Client**.

> ***Note***: Other DocuSign Signature Appliance components will appear in the list of components to uninstall, however, select to uninstall only the **DocuSign Signature Appliance Client**.and this will uninstall all related components.

3. The following screen appears. Click **Remove** to uninstall. The uninstall process begins.

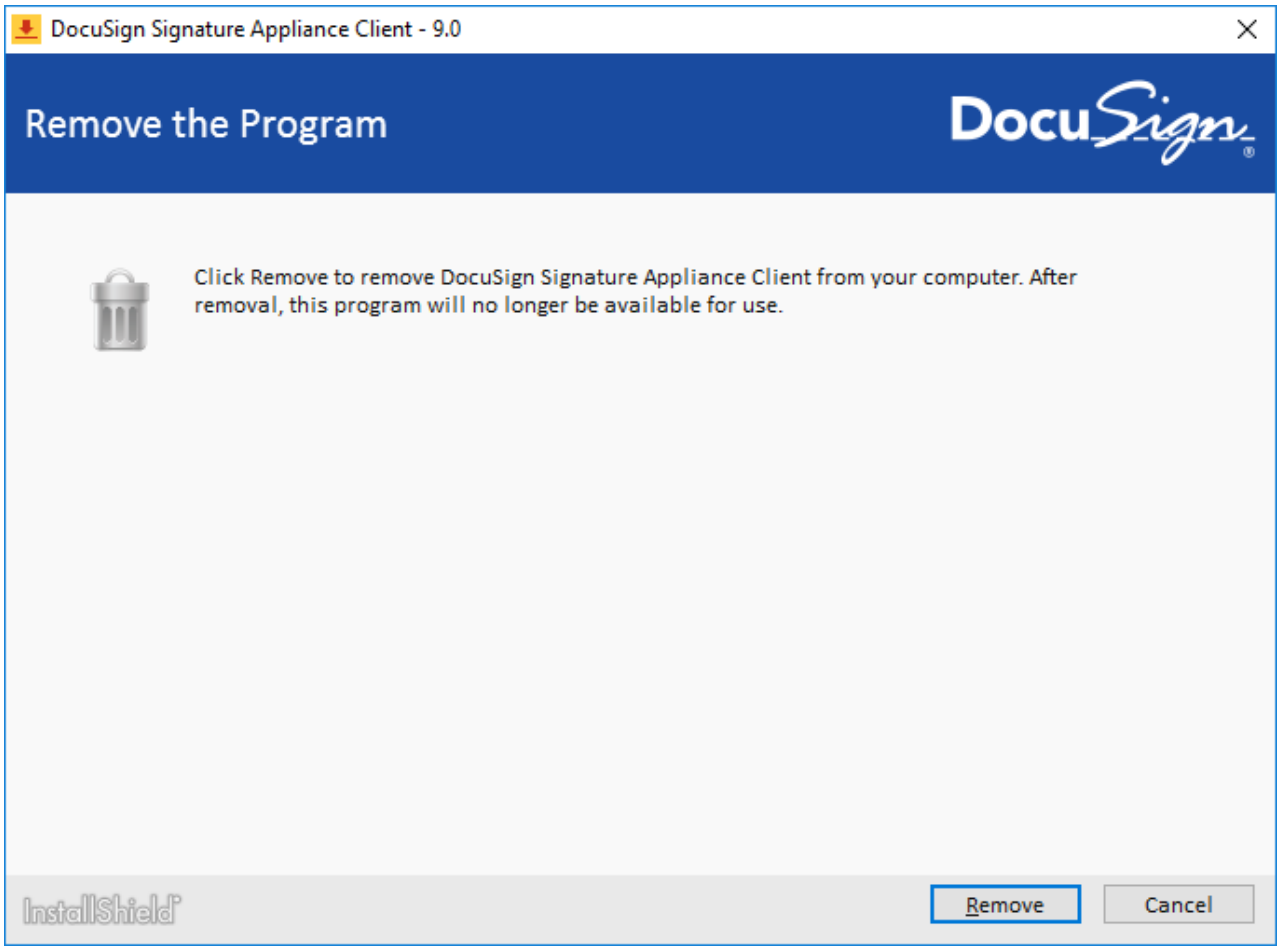


Figure 51 Removing the DocuSign SA Client

4. When the DocuSign SA Client is uninstalled from the workstation, a screen appears to inform you that the system finished uninstalling. Click **Finish**.

The DocuSign SA client is uninstalled from the workstation.

Uninstalling the Client in an Active Directory Environment

Refer to *Appendix* B: Centralized DocuSign SA Client Installation for information on how to centrally instruct all clients to uninstall their DocuSign SA client installation.

Distributing DocuSign SA Information through the SCP

The DocuSign SA 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 SA 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 SA 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 SA client with the necessary information using the Configuration Utility (refer to *Chapter 8: DocuSign SA Configuration Utility*). If you wish, you can also use the Configuration Utility to manually configure each DocuSign SA 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 DocuSign SA Client Installation.

Microsoft Active Directory SCP

To view the DocuSign SA SCP in a Microsoft Active Directory:

1. In the DocuSign SA 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 SA Service Connection Point For CSN00001* where CSN0001 is the specific DocuSign SA serial number.

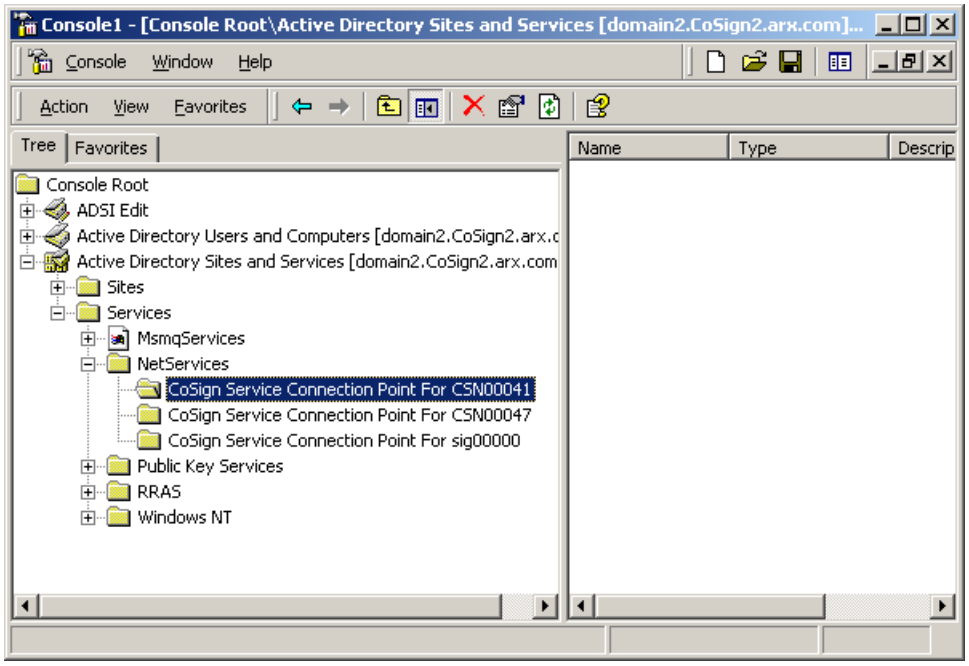


Figure 52 Active Directory SCP

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):

- DocuSign SA IP address.

- DocuSign SA listening port number.
- DocuSign SA availability status (**Up** or **Down**).

> ***Note:*** In rare cases where the DocuSign SA 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*.

- DocuSign SA `prompt for logon` parameter value – Directs the client whether to present a logon popup window for accessing DocuSign SA, or whether to use Microsoft mechanisms.
- DocuSign SA `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 SA clients will not attempt to connect to irrelevant appliances.

Using the DocuSign SA Client System Tray Icon Options

All client-based operations are activated through the right-click menu options of the DocuSign SA Client system tray icon . Refer to the *DocuSign Signature Appliance User Guide*.

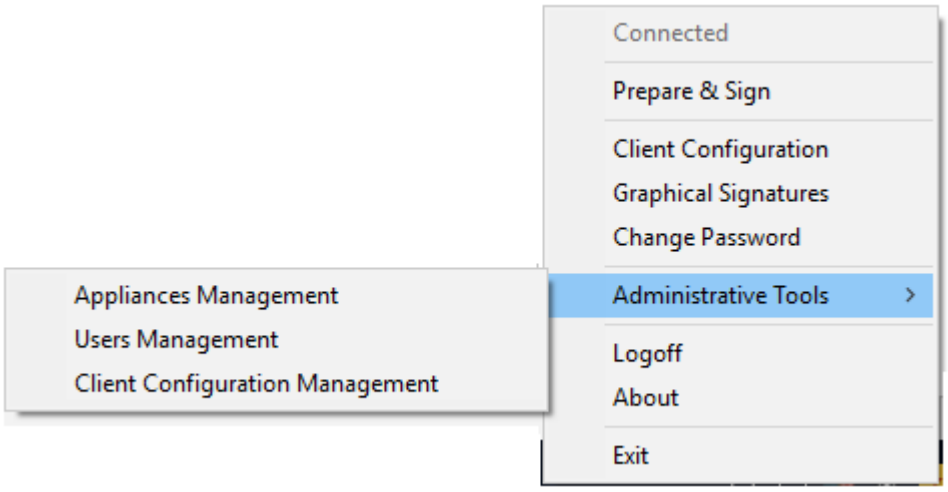


Figure 53 Right-click menu options of the DocuSign SA client system tray icon

Administrator Actions

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

Appliances Management – This option displays the DocuSign SA Administration MMC. Using the DocuSign SA Administration MMC it is possible to install or restore the appliance, or manage

it in operation mode. Refer to *Chapter 3: Installing DocuSign SA* and *Chapter 5: Managing the DocuSign Signature Appliance* for more information related to the DocuSign SA Administration MMC.

Users Management – This option activates the DocuSign SA Users Management application. This application is mandatory when DocuSign SA 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 DocuSign SA Configuration Utility in administrative mode. For more information, refer to *Chapter 8: DocuSign SA Configuration Utility*.

Installing the Root Certificate

In order to sign or validate documents originating from an organization, you must install on your workstation the organization's DocuSign SA ROOT certificate.

For a full explanation of how to install a ROOT certificate, refer to the section *Installing the Root Certificate* in the *DocuSign SA 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.

Adding the certificate chain if DocuSign TSCP CA is used

If DocuSign TSCP CA is used, make sure you add all certificates in the certificate chain in addition to the end user certificate. You need to load the following (refer to *Installing Certificate Chains* in the *DocuSign SA User Guide)*:

- TSCP SHA256 Bridge CA
- DocuSign Root CA

- DocuSign General CA

Adding the certificate chain if DocuSign CA is used

If DocuSign CA is used, make sure you add all certificates in the certificate chain in addition to the end user certificate. You need to load the following (refer to *Installing Certificate Chains* in the *DocuSign SA User Guide)*:

- DocuSign Private CA

Extended Authentication Mode

DocuSign SA enables the use of an extended authentication mode, 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 an additional device such as an OTP device.
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 SA 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 SA supports a maximum password length of 128 characters.
- *OTP based on an internal OTP mechanism* **–** The end user is prompted to provide the OTP during the digital signature operation.
  An OTP shared secret that is unique for every user is downloaded to the OTP device (such as a mobile phone) as part of an enrollment stage.
  The OTP mechanism is based on a time-based OTP (OATH-TOTP standard).
  For more information about the various parameters that require configuration in order to interface to the RADIUS server, refer to *Extended Authentication*.
  Note: DocuSign SA supports a maximum password length of 128 characters.
- If DocuSign SA is operating in Common Criteria EAL4+ mode, OTP is used for every digital signature operation. The OTP is validated by the DocuSign Signature Appliance.
  In the case where a Radius Server is deployed, additional integration is required within the Radius Server for interacting with the DocuSign Signature Appliance for the purpose of OTP validation. For information, contact DocuSign.

To configure DocuSign SA to use extended authentication, refer to *Extended Authentication*.

Chapter 5: Managing the DocuSign Signature Appliance

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

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

Note: Managing DocuSign SA 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 DocuSign SA Administration MMC

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

1. You must be the built-in administrator defined during DocuSign SA installation;

   Or

   You must belong to the domain's administrative group as well as a valid DocuSign SA user. For example, in a typical Active Directory installation, you must belong to the DocuSign SA 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 SA Admin appliance management rights.

2. Before performing any appliance administrative activity, you must manually login to DocuSign SA using either the built-in administrator or another valid administrator account.

Starting the DocuSign SA Administration MMC

To start the DocuSign SA Administration MMC:

1. In the system tray, right-click the  icon and select **Administrative Tools → Appliances Management**.

   The *DocuSign Signature Appliance Management* window appears, showing all installed DocuSign Signature Appliances (*Figure 54*).

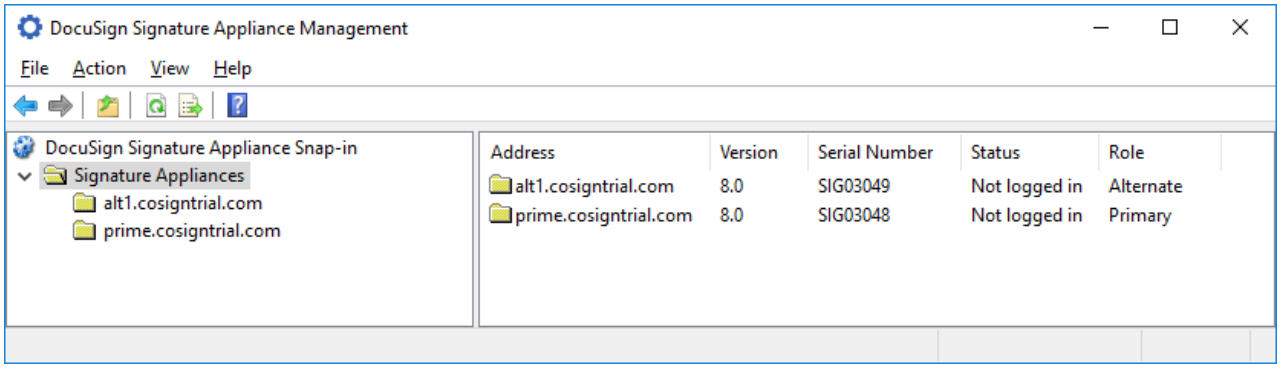


Figure 54 DocuSign Signature Appliance Management Window

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

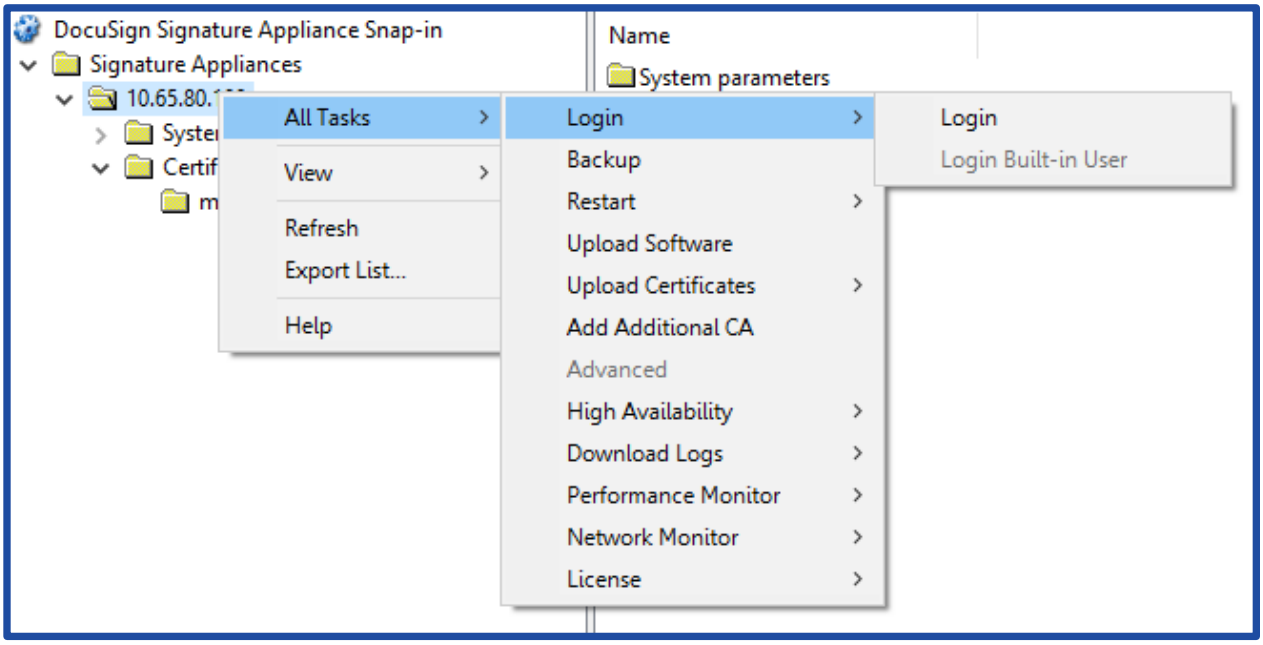


Figure 55 DocuSign Signature Appliance Management Window – Logging in to DocuSign SA as an Appliance Administrator

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

DocuSign SA Administration MMC Capabilities

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

- Back up the current DocuSign SA data.
- Shut Down and Restart DocuSign SA Service.
- Restart the DocuSign Signature Appliance.
- Upload software updates provided by DocuSign.
- Upload a new SSL Server certificate to be used as part of the DocuSign SA Web Services offering. This operation is also relevant if the DocuSign SA Web Services interface that is based on Rest API is used.
- Configure high availability options.
- Download log files from the DocuSign Signature Appliance.
- 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.
- Manually synchronize DocuSign SA with your Microsoft Active Directory or LDAP directory.
- Manage multiple CAs of the Appliance and change their parameters.
- Synchronize DocuSign SA with the External CA. This option is relevant when DocuSign SA is interfacing with an external CA automatically for producing users' certificates.
- Refresh Certificates.
- View and modify system parameters.
- Restore the DocuSign Signature Appliance from backup data.
- Install a new DocuSign Signature Appliance (refer to *Installing the DocuSign Signature Appliance Software*).
- Install an alternate DocuSign Signature Appliance (refer to *Installing an Alternate DocuSign Signature Appliance*).

Backing up the DocuSign SA Data

You can back up the entire DocuSign SA database (which includes all the users' keys, CAs' information, Groups' information, Users' certificates and graphical signatures), and all the DocuSign SA 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 SA 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 DocuSign Signature Appliance*.

Note: You cannot backup the Appliance if DocuSign TSCP CA is used.

To back up the DocuSign SA database:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the DocuSign Signature Appliance you wish to back up.
2. From the popup menu, select **All Tasks** → **Backup**. The Select a File dialog box appears.
3. Select a local backup file and click **Save**. The DocuSign SA 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*).

Shutting Down and Restarting DocuSign SA Services

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

To stop and then restart the DocuSign SA services:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance.
2. From the popup menu, select **All Tasks → Restart → Soft Restart**.

Restarting the DocuSign Signature Appliance

There are several options for restarting or shutting down DocuSign SA 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 DocuSign Signature Appliance:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance.
2. From the popup menu, select **All Tasks** → **Restart** → **Hardware Restart/Shutdown Appliance**.

Upgrading DocuSign SA

You can upload DocuSign SA 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 DocuSign SA Console's **Status** tab to verify the existing appliance software version (refer to *Displaying DocuSign Signature Appliance Status*).

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 SA 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 8.5

To upgrade from version 8.4 to version 8.5:

1. Load `verupd85.dlm` from the DocuSign SA version 8.5 CD.
2. Follow the instructions listed in *Uploading a Software Update*. The upgrade runs immediately.
3. Use the DocuSign SA Console's **Status** tab to verify that the software version is `Software Version 8.5`. (refer to *Displaying DocuSign Signature Appliance Status*).

Upgrading to Version 8.51 (system upgrade)

To upgrade from version 8.5 to version 8.51:

1. Load `DSAWinU3.dlm` from the DocuSign SA version 8.51 CD.
2. Follow the instructions listed in *Uploading a Software Update*. The upgrade runs immediately.
3. Use the DocuSign SA Console's **Status** tab to verify that the software version is `Software Version 8.51.9.0`. (refer to *Displaying DocuSign Signature Appliance Status*).

Upgrading to Version 9.0

To upgrade from version 8.51 to version 9.0:

1. Load `verupd90.dlm` from the DocuSign SA version 9.0 CD.
2. Follow the instructions listed in *Uploading a Software Update*. The upgrade runs immediately.
3. Use the DocuSign SA Console's **Status** tab to verify that the software version is `Software Version 9.0.9.10`. (refer to *Displaying DocuSign Signature Appliance Status*).

Upgrading to Version 9.1

To upgrade from version 9.0 to version 9.1:

1. Load `verupd91.dlm` from the DocuSign SA version 9.1 CD.
2. Follow the instructions listed in *Uploading a Software Update*. The upgrade runs immediately.
3. Use the DocuSign SA Console's **Status** tab to verify that the software version is `Software Version 9.1.9.10`. (refer to *Displaying DocuSign Signature Appliance Status*).

Upgrading to Version 9.3

To upgrade from version 9.1 to version 9.3:

1. Load `verupd93.dlm` from the DocuSign SA version 9.3 CD.
2. Follow the instructions listed in *Uploading a Software Update*. The upgrade runs immediately.
3. Use the DocuSign SA Console's **Status** tab to verify that the software version is `Software Version 9.3.9.20`. (refer to *Displaying DocuSign Signature Appliance Status*).

Uploading a Software Update

To upload a software update:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the DocuSign Signature Appliance to which you wish to upload the software.
2. From the popup menu, select **All Tasks** → **Upload Software**. The Select a File dialog box appears.

3. Select a local software update file and click **Open**. The DocuSign SA 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 SA's console or view the log files to validate the success of the operation.

Additional Security related updates

Use the following update (.dlm files) to enhance/change security related features of the DocuSign Signature Appliance. The DLM files are located in the `SecDlms` directory in the DocuSign SA Client CD.

To upload the DLMs, follow the instructions listed in *Uploading a Software Update*.

Note: When DocuSign SA is deployed in Common Criteria EAL4+ mode, uploading the following updates/changes is mandatory.

DisWPAD.dlm:

Use this DLM to disable outgoing DNS multicast messages and other mechanisms that are part of the WPAD (Web Proxy Auto Discovery) protocol.
WPAD may be maliciously used to explore some non-critical information that is transmitted by the DocuSign SA. Therefore, in cases where WPAD is not required, it is highly recommended to deploy this DLM.

SHA256: **9366425ba4c0e7f67e13d161edb9ef0efda902c90042889e0cddfb94e05848b0**

Replacing the manufacturing DSA server certificate:

If you wish to change the manufacturing DocuSign Signature Appliance TLS certificate, please contact DocuSign Support.
The existing certificate is based on a SHA1 RSA based signature, but it is possible to change the certificate to include a SHA256 RSA based signature.
The provided replacement file will be a dedicated DLM file.

It is important to keep in mind that this DLM file should be uploaded to the Appliance before the installation of the Appliance.

Uploading Certificate material to DocuSign SA

You can upload required certificates (normally ROOT certificates) or SSL Server Certificates to DocuSign SA.

Upload certificates

To upload ROOT certificates and intermediate CA certificate to DocuSign SA:

1. Right-click the relevant **DocuSign Signature Appliance** and select **All Tasks** → Upload Certificates → Upload **ROOT Cert**ificate **Chain**.

   A file selection window pops up.

2. 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.**

Uploading an SSL Certificate

If DocuSign SA 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* or *www.cosign.com*, depending on the Appliance's version. This default certificate would require that the organization configure each client as follows:

- Assign DocuSign SA's IP address to the name *cosign* or *www.cosign.com*. (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:

1. Generate a private key and request a certificate from a well-known certificate authority.
1. Upload the Private Key and Certificates chain that are packaged in a .pfx file to the DocuSign Signature Appliance.
2. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance, and select **All Tasks** → **Upload Certificates** → **Upload SSL Certificate**
3. A window appears, requesting you to supply the following:

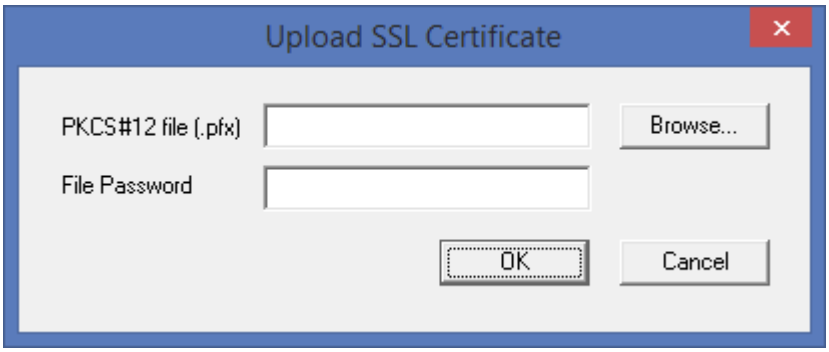


Figure 56 Upload SSL Certificate

- **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.

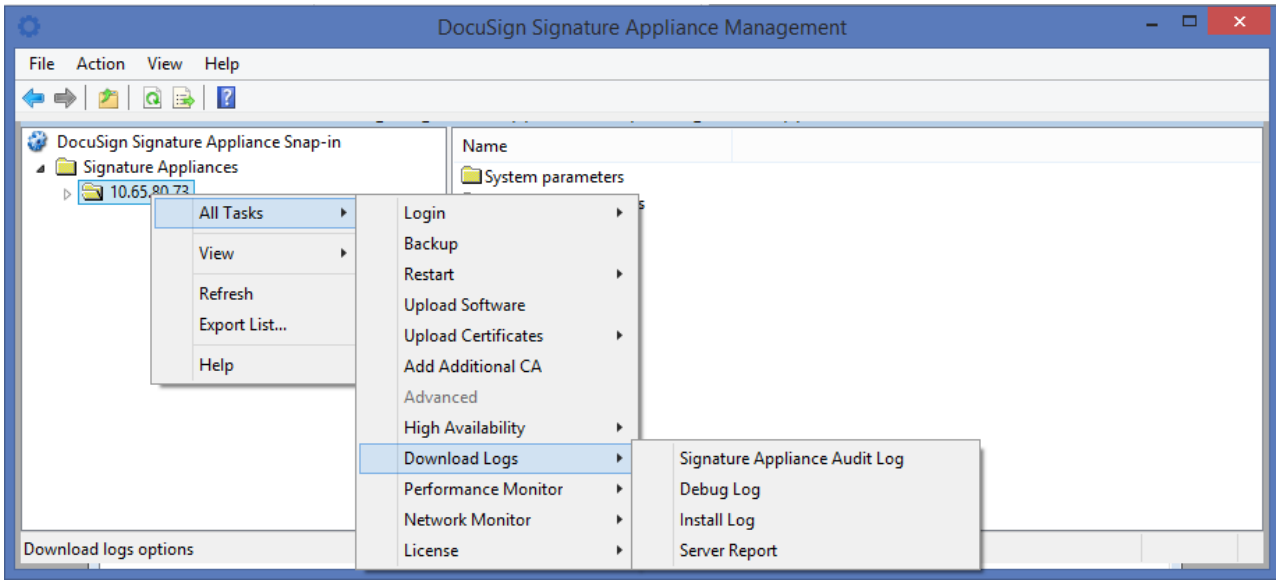
High Availability

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

- **Install Alternate** – Install the alternate DocuSign Signature Appliance software. Refer to *Installing the Alternate DocuSign Signature Appliance Software*.
- **Subscribe Alternate to Primary** – Re-subscribe an existing installed appliance to be an alternate appliance of a selected primary appliance. Refer to *Re-subscribing 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*
- **Set replication communication mode** – Set communication between the Primary Appliance and alternate appliance to be based on an IPSEC non-IKE communication that is a FIPS 140-2 approved mechanism. Refer to *Setting the Communication Protocol between the Primary Appliances and Alternate Appliances*.

Downloading Log Files

There are four types of DocuSign SA log files that you can download:



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

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

The DocuSign SA Audit Log is managed inside the appliance database. Upon a request to retrieve the audit 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 DocuSign SA 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. See the following table for a full list of all possible event IDs.
- Value – A textual description of the event. See the following table for a full list of all possible events.
- SignedData – In the case of a digital signature operation, this value is the hash representation of the data to be signed.

To view the Audit log:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance.
2. From the popup menu, select **All Tasks** → **Download Logs** → **Signature Appliance Audit Log**.
3. Select a file and click **OK**.
4. Unzip the file to obtain a .CSV file.
5. Use an application such as Excel or Notepad to view the .csv file.

Note: You can also download DocuSign SA's Audit log by using the command line utility `GetEvt` (refer to *Using Command Line Utilities*).

Note: The Audit log can be downloaded also from the alternate appliance. Each appliance manages its own events, and events are not copied automatically between appliances.

The following table lists all possible Audit log entries:

Event ID	Description
1	Backup appliance
2	Restart appliance
3	Add alternate appliance
4	Remove alternate appliance
5	Reset alternate appliance
6	Configure alternate appliance as master
7	Remove publication from appliance
8	Get install log
9	Get debug log
10	Get event log

Event ID	Description
11	Get performance log
12	Start performance monitor
13	Stop performance monitor
14	Set system parameter
15	Upload dlm
16	Load SSL certificate
17	Set CA parameters
18	Get CA parameters
19	Load root CA chain
20	Start full CA sync
21	Start full users sync
22	Start full users refresh
23	Enforce users certificate refresh
24	Enforce users certificate refresh success
25	Enforce users certificate refresh failed
26	Start sync task
27	Get CRQ
28	Start loading CRP
29	Change password to user
30	Reset user password counter
31	Admin login
32	Authentication failure
33	Signing key revocation
34	Signing key generation
35	Signing key certificate upload
36	Account activation

Event ID	Description
37	Account already activated
38	Change password
39	Administrator enable user
40	Administrator disable user
41	Assign user to group
42	Reset tamper
43	Enroll CoSign user
44	Renew CoSign user certificate
45	Revoke CoSign user
46	User signed data
47	Detect tamper
48	Can't refresh certificate, CA about to expire
49	Reached 90% of CoSign license limit
50	License limit has been reached
51	License is about to expire
52	Appliance license is not present
53	Appliance users amount passed the license limit
54	License is expired
55	An improper license mini-key is inserted
56	Bound to new DC
57	Full directory synchronization success
58	Full directory synchronization failed
59	Delete RSA key from pool failed
60	License number of transactions exceed maximum
61	Get console log
62	Exceed maximum users for automatic refresh certificates

Event ID	Description
63	Get network monitor log
64	Start network monitor
65	Get dump files

Note:

- Event number 10 relates to downloading the audit log.

- Event number 15 relates to uploading a software update.

To download the Server Report:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance.
2. From the popup menu, select **All Tasks** → **Download Logs** → **Server Report**.
3. Select a file and click **OK**.

   The report is a text file containing the following sections:

   - General Appliance information, including its IP address, Hardware version and Software version.
   - The values of all the Appliance's System parameters.
   - Number of users and values of System Signature Counters.
   - Information displayed in the Appliance's Web Console.

Renewing the DocuSign CA's RA certificate

When using DocuSign TSCP CA or DocuSIgn CA as the automatic external CA, the DocuSign Signature Appliance is authenticated to the DocuSign CA service using an authentication key and an authentication certificate. When the authentication certificate expires, it is required to regenerate the authentication key and get a new certificate. This process occurs every three years.

To renew the DocuSign CA's RA authentication key and certificate:

4. In the DocuSign Signature Appliance Management window (Figure 57), right-click the relevant DocuSign Signature Appliance and select the default CA in the **Certificate Authorities** section. Then select **all Tasks → Download RA certificate request.**

   A new DocuSign CA's RA certificate request is downloaded.

5. Send the certificate request to DocuSign.

   DocuSign will reply with a new certificate.

6. In the DocuSign Signature Appliance Management window (Figure 57), right-click the relevant DocuSign Signature Appliance and select the default CA in the **Certificate Authorities** section. Then select **all Tasks → Upload RA certificate reply.**

   The Upload CA Information window appears:

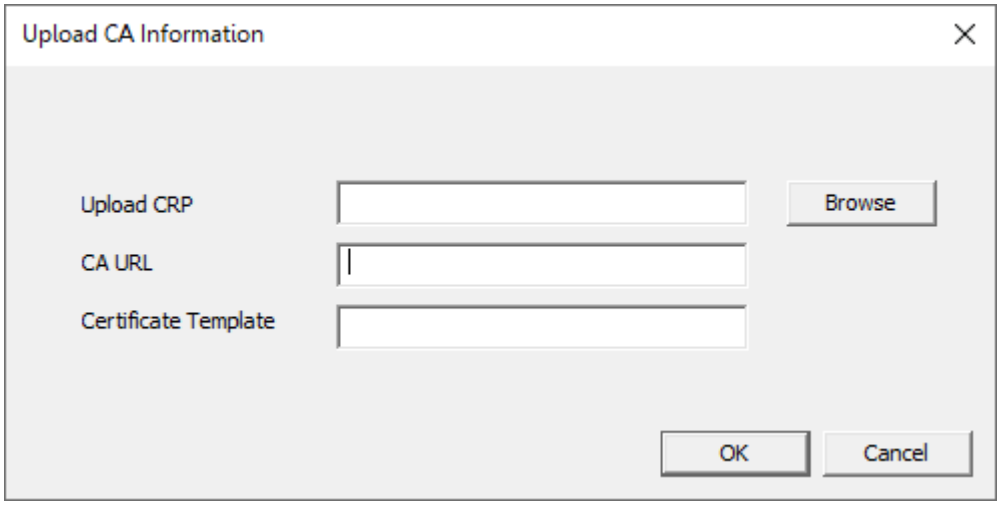


Figure 57 Upload CA Information Window

7. Enter the following information, and then click **OK**:

   - **Upload CRP** – Browse to the authentication certificate file provided by the DocuSign. The default file name is *RA-certificate.pfx*.
   - **CA URL** – Enter the URL of the CA as provided to you by DocuSign.
   - **Certificate Template** – Enter the the identity of the Certificate template as provided to you by DocuSign.

8. Click **OK**.

   As part of the operation, the Appliance will communicate with DocuSign CA.

A success message appears, indicating that communication with DocuSign CA is successful.

Renewing the Symantec Authentication Key File

When using Symantec as the automatic external CA, the DocuSign Signature Appliance is authenticated to the Symantec service using an authentication key and an authentication certificate that are uploaded to DocuSign SA as part of the DocuSign SA installation process.

Close to the expiration date of the authentication key, you should logon to the Symantec portal using your organizational account, and request to renew the authentication key. To do so, repeat the exact process you following when installing the appliance. Refer to *Using an External CA in Automated Mode – Symantec*.

By default, the Account Name and Account profile ID of the new Symantec key will be those appearing in DocuSign SA's authentication PFX file the last time it was uploaded.

To renew the Symantec authentication key file when using Symantec as the automatic external CA:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Upload CA Information.**

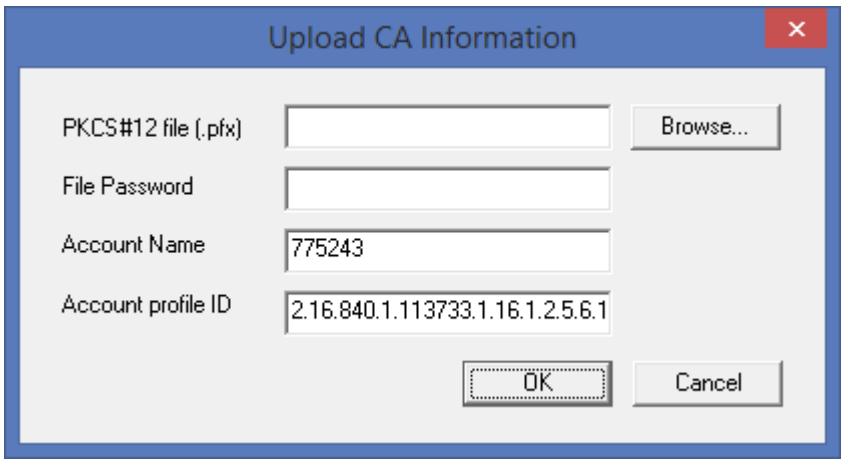


Figure 58 Upload CA Information Window populated with Symantec Account Name and Account Profile ID

Monitoring Performance Parameters of the DocuSign Signature Appliance

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

Activating Performance Monitoring

To monitor appliance performance parameters:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Performance Monitor → Start Monitor.** The Setup Performance Monitor Parameters window appears.

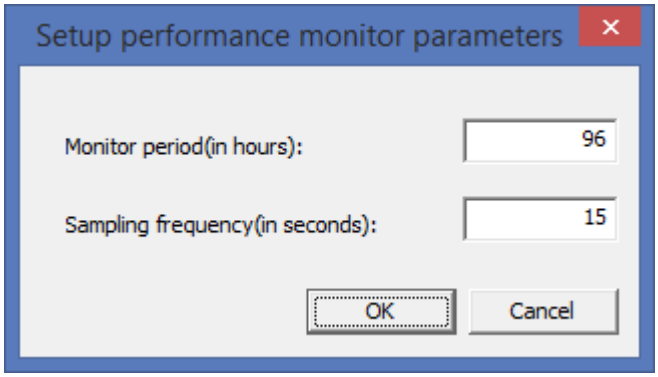


Figure 59 Setup Performance Monitor Parameters Window

2. 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.
3. 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:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Performance Monitor → Stop Monitor**.

Viewing Performance Parameters

To view the appliance performance parameters:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Performance Monitor → Download Log**.

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

Monitoring Network Packets to/from the DocuSign Signature Appliance

Note: Please use this functionality only if requested to do so by the DocuSign Support team.

In rare cases, you may be instructed by the DocuSign Support team to capture networking information as part of an analysis of a network connectivity problem.
The Capture operation triggers a networking packet capturing mechanism that collects networking packets for several minutes. After packet capturing is complete, the information can be downloaded by the Appliance Administrator to the administrative client for further analysis.

Activating Network Capturing

To start capturing networking packets:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Network Monitor → Start Monitor.** The Setup Network Monitor Parameters window appears.

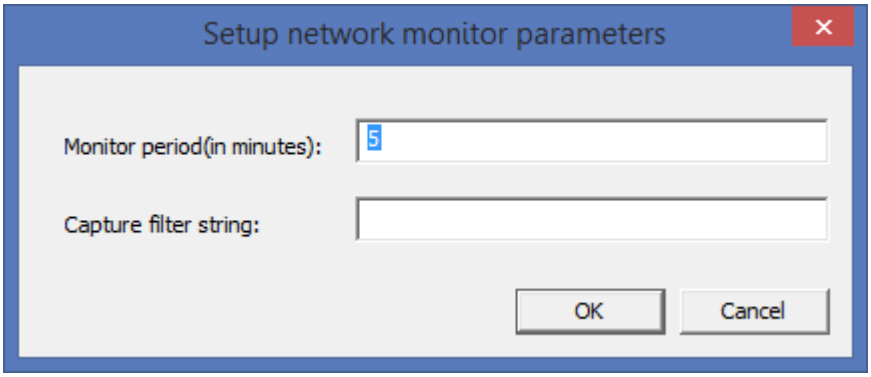


Figure 60 Setup Network Monitor Parameters Window

2. Specify the following:
   - **Monitor period (in minutes)** – Specify the length of the network capturing period. When the capturing period ends, the networking capturing service will stop.
   - **Capture filter string** – Leave this field empty or follow any other instruction given by DocuSign Support.
3. Click **OK**.

Networking capturing begins. Monitoring will end at the end of the specified period, or if you manually stop it as described in *Stopping Performance Monitoring*.

Stopping Network Capturing

To stop capturing networking packets:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Network Monitor → Stop Monitor**.

Downloading captured networking packets

To download the captured networking packets:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Network Monitor → Download network monitor file**.

The downloaded file contains all captured packets compressed in a .gz file format. Extract the *netmon.pcap* file and use any network analysis tool to view its contents.

Obtaining a New DocuSign SA License

You can obtain a new DocuSign SA 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:

1. Make sure the license token is plugged into the USB slot in the DocuSign Signature Appliance.
2. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → License → Download License Request.**

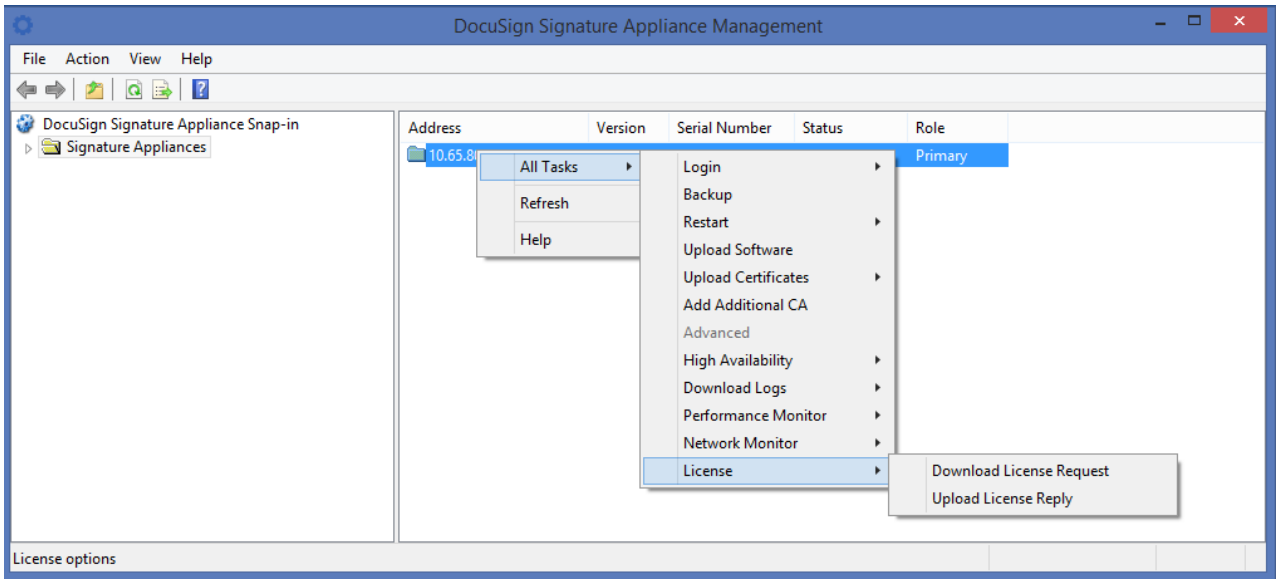


Figure 61 License Options

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

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

Uploading the New License

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

To upload the new license:

1. Save the new .lmu license file on your system.
2. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → License → Upload License Reply** (Figure 61).
3. Specify the .lmu license file.

   The new license file is uploaded to the license token.

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

Advanced Options for Active Directory or LDAP Deployments

Follows some several new administrative features for performing advances operations related to Active Directory deployment.

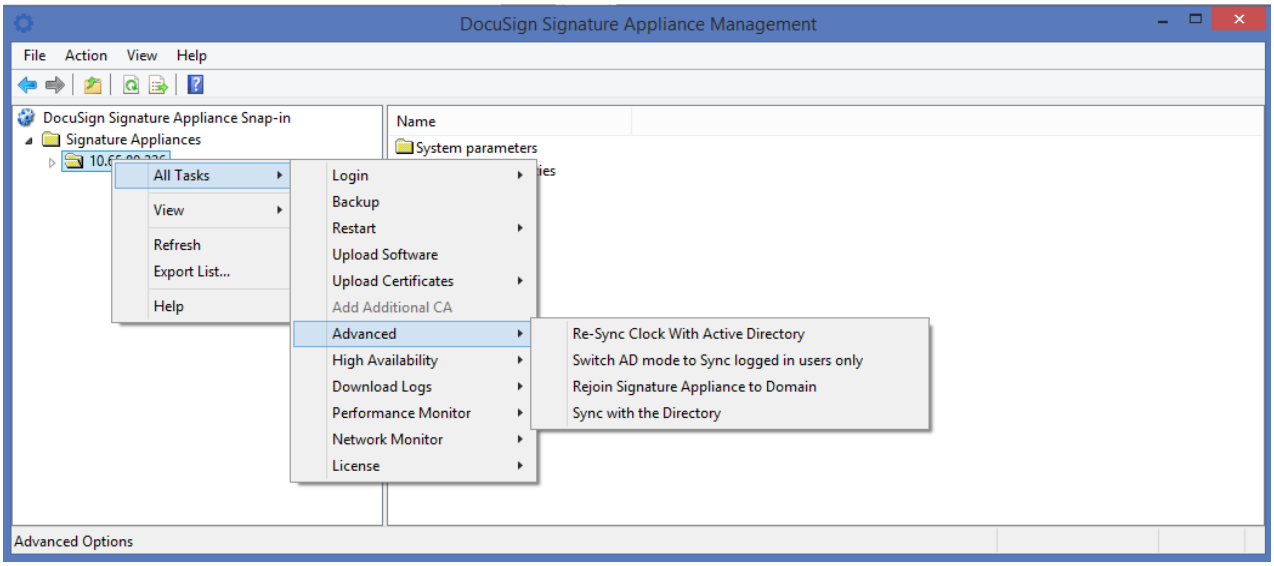


Figure 62 Advanced Options

Resyncing the Appliance Clock with Active Directory

Use the following option to re-synchronize the Appliance clock with Active Directory

To re-sync the Appliance clock with Active Directory:

1. Log on as Appliance administrator, using the built-in Administrator.
2. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Advanced → Re-Sync Clock with Active Directory** (*Figure 62*).
3. A confirmation message appears. Click **OK** to resync the clock.

Changing a regular Active Directory deployment to Multiple Domain deployment

The following option should be performed with care. It is highly advisable to perform an Appliance Backup before performing this operation.
Use the following option to change the deployment of the Appliance from a regular Active Directory to a Multiple Domain deployment

To change the Appliance deployment from regular Active Directory to Multiple AD domain:

1. Log on as Appliance administrator, using the built-in Administrator.

2. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Advanced → Switch AD mode to Sync logged in users only** (*Figure 62*).
3. A confirmation message appears. Click **OK** to perform the configuration change.

In a high availability setup, the configuration change should be made in the Primary appliance. Once the configuration change is completed, the Alternate Appliances should be hardware restarted.

Re-Joining an Appliance to the AD Domain

The following option should be performed with care. It is highly advisable to perform an Appliance Backup before performing this operation.
Use the following option to rejoin the Appliance to the Active Directory Domain.

To rejoin the Appliance to the AD Domain:

1. Log on as Appliance administrator, using the built-in Administrator.
2. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the relevant DocuSign Signature Appliance and select **All Tasks → Advanced → Rejoin Signature Appliance to Domain** (*Figure 62*).
3. A confirmation message appears. Click **OK** to perform the rejoin operation.

Synchronizing DocuSign SA with the Directory Service

This option can be used on either Active Directory deployments or LDAP deployments.

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

DocuSign SA monitors and retrieves information directly from the directory service.

During DocuSign SA installation, the DocuSign SA 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 SA 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 SA 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 SA automatically generates a new certificate for the user. In this way, DocuSign SA and the directory service remain synchronized.

In certain cases, however, DocuSign SA may lose synchronization with the directory service. This may occur if you run DocuSign SA 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 SA with the directory service.

Another case requiring manual synchronization of the directory is the case where an Active Directory environment is used, and DocuSign SA 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 SA 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 SA, but if it is required to remove these users from DocuSign SA, it is necessary to perform the manual synchronization operation.

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

Note: If DocuSign SA 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 DocuSign SA System Parameters*).

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

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

To manually trigger synchronization of DocuSign SA with the directory service:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance, select **Certificate Authorities**, right click the relevant CA, and 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?`

2. 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 Audit log indicates when the operation is complete.

Managing Certificate Authorities in the DocuSign Signature Appliance

Starting from DocuSign version 8.5, it is possible to define and associate multiple Certificate Authorities with a specific DocuSign Signature Appliance, and map users to different certificate authorities.

Once a new CA is defined, you can setup various parameters for the newly created CA.

Adding a new CA

Note: Keep in mind that once a new CA is added, it is impossible to delete it. Therefore, do not create test CAs once your system is in production.

To add a new CA:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), right-click the desired DocuSign Signature Appliance.
2. From the popup menu, select **All Tasks** → **Add Additional CA**. The *CA setup* screen appears.

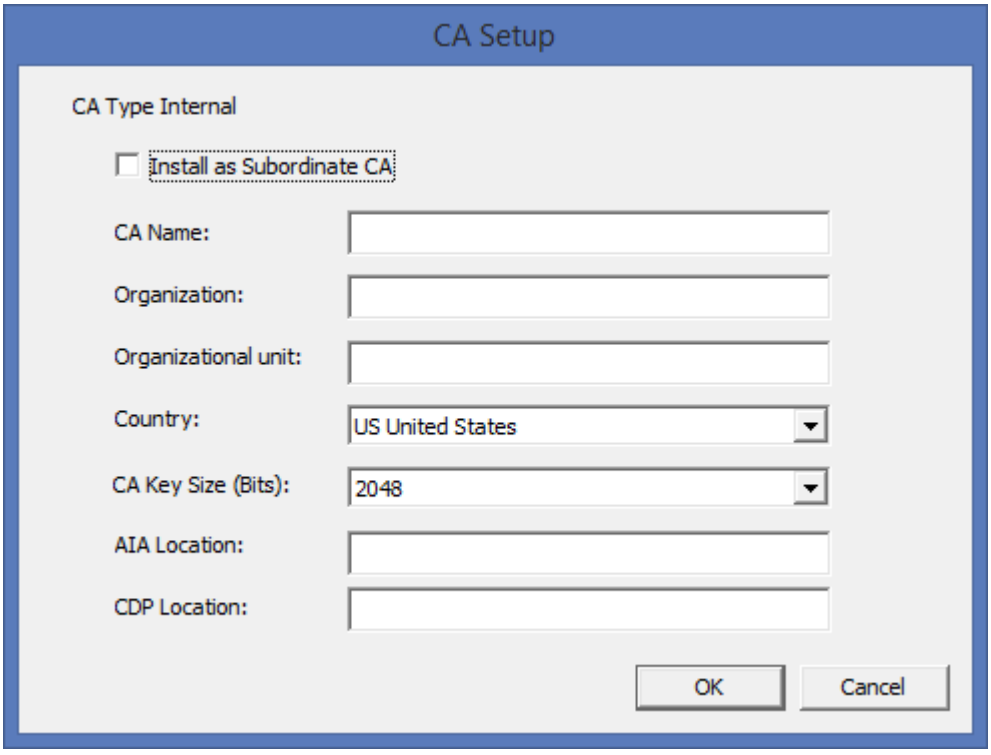


Figure 63 CA Setup window

3. Specify **Internal CA** in the **CA type** field.
4. Enter the following information:
   - **Install as Subordinate CA** – Select this option if you wish to install the DocuSign SA CA as a subordinate CA.

You can install the DocuSign SA 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 SA 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.

- **CA name** – The identifying name of DocuSign SA'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 and also in the user 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 and in the user certificate.
- **CA key size (bits)** – The size of the key of the CA.
- **AIA Location** – AIA (Authority Information Access) is put into the end user's certificate and specifies where the DocuSign SA 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 SA..

  The default value in the case of Active Directory includes the LDAP location. If the default is not modified, the DocuSign SA installation will also put the DocuSign SA 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 DocuSign SA 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 SA.

  The default value in the case of Active Directory includes the LDAP location. If the default is not modified, DocuSign SA 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 SA AIA and CRL, refer to *Changing DocuSign SA System Parameters*.

Managing the list of CAs

Using the *DocuSign Signature Appliance Management* utility you can manage the list of deployed CAs.

To manage the list of deployed CAs:

- In the DocuSign Signature Appliance Management window, right-click the desired DocuSign Signature Appliance, and select **Certificate Authorities**.

  All created CAs appear.

  The default CA instance is the CA that was created during Appliance installation. It is marked by the addition of **(default)** in the GUI.
  Only the default CA can be configured to interact with external CAs in automated mode.

  The other CAs can be internal CAs or internal CAs configured as subordinate CA.

Synchronizing DocuSign SA with the External CA in Automated mode

Note: This operation is not relevant when DocuSign SA 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 SA database and the external CA.
This option can be used when interfacing with the DocuSign external CA or DocuSign TSCP CA or Symantec CA.

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

To synchronize DocuSign SA with the external CA:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), select the relevant DocuSign Signature Appliance, select **Certificate Authorities**, right-click the relevant CA with whom you wish to synchronize, and 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 SA, is revoked.
   - For every user in DocuSign SA 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 SA.

Refreshing Certificates

> ***Note:*** This operation is not relevant when DocuSign SA 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:

1. In the DocuSign Signature Appliance Management window (*Figure 54*), select the relevant DocuSign Signature Appliance, select **Certificate Authorities**, right click the relevant CA whose users' related certificate you wish to refresh, and from the popup menu, select **All Tasks → Synchronize → Full User Certificates refresh**.

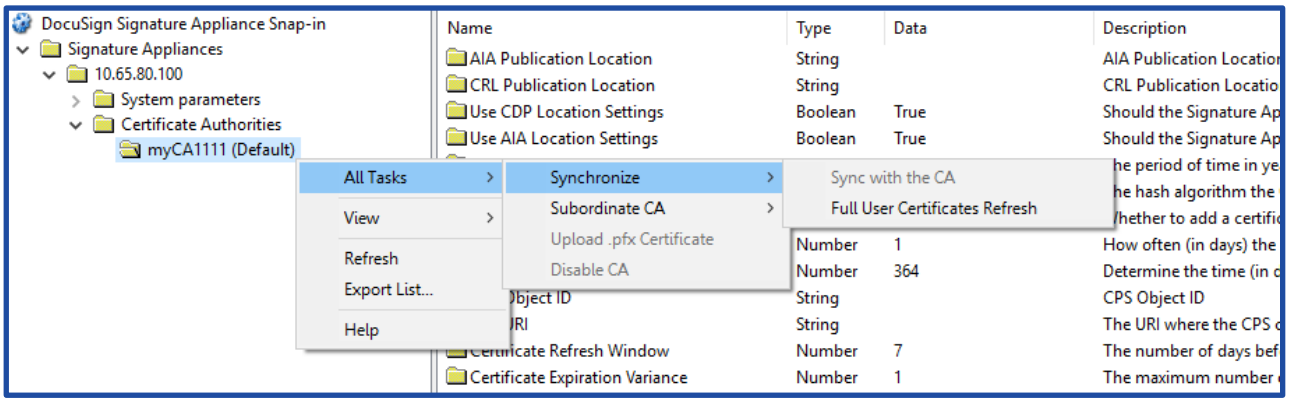


Figure 64 Selecting Full User Certificates Refresh

2. Confirm the operation.

Following synchronization:

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

> ***Note:*** The **Full User Certificates Refresh** option is relevant also when DocuSign SA interfaces an external CA automatically. Keep in mind that this option will generate new certificates for all users.
>
> ***Note:*** When DocuSign TSCP CA or DocuSign CA are deployed, the **Full User Certificate Refresh** option is located directly under **All Tasks**.

Renewing the Subordinate CA Certificate

> ***Note:*** This operation is not relevant when DocuSign SA is deployed in a Common Criteria EAL4+ mode of operation.

It is possible to install DocuSign SA so that DocuSign SA acts as a subordinate CA of another ROOT CA in the organization's environment. For more information on installing DocuSign SA as a subordinate CA, refer to *Installing DocuSign SA as a Subordinate CA*.

If the DocuSign SA certificate from the ROOT CA has expired or been revoked, you need to renew the DocuSign SA 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 DocuSign SA certificate when the Appliance's CA is acting as a subordinate CA:

1. In the DocuSign Signature Appliance Management window (*Figure 65*), select the relevant DocuSign Signature Appliance, select **Certificate Authorities**, right click the relevant CA for whom you wish to get a certificate request, and select **All Tasks → Subordinate CA → Download Certificate Request (.crq)**

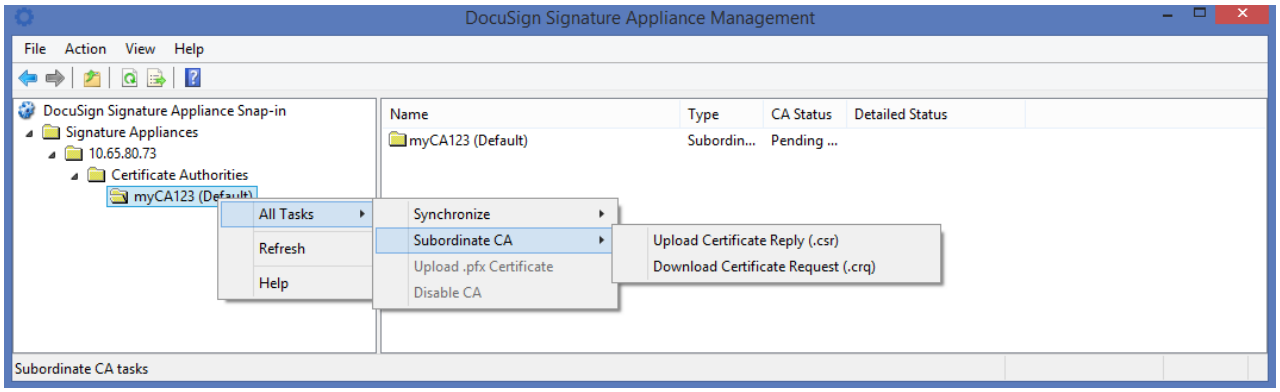


Figure 65 Subordinate CA Options

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

   DocuSign SA will place the CRQ into this file.

3. 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 DocuSign SA subordinate CA certificate.
   Note that if a ROOT CA certified DocuSign SA, the complete chain of CA certificates includes only the ROOT CA certificate.
   The DocuSign SA 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 DocuSign SA 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 SA 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.

4. For each file in the chain of CA certificates, perform the following:

   - Right-click the relevant **DocuSign Signature Appliance** and select **All Tasks → Upload Certificates → Upload ROOT Certificate 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.**

5. Select the relevant DocuSign Signature Appliance, select **Certificate Authorities**, right click the relevant CA whose certificate reply you wish to upload, and select **All Tasks → Subordinate CA → Upload Certificate Reply (.csr)**

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

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

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

Disabling a CA

A CA that is not relevant anymore can be disabled. You can disable a CA only if there are no users bound to the CA.

The only operations you can perform on a disabled CA is to download its CRL or get an OCSP response for such a CA.

To disable a CA:

- Select the relevant DocuSign Signature Appliance, select **Certificate Authorities**, right click the relevant CA and select **All Tasks → Disable CA**.

  A confirmation message requests that you confirm the operation.

  A disabled CA cannot be re-enabled.

Setting CA parameters

In the Administration MMC, you can set the following system parameters for each CA in the list of CAs by selecting the specific CA in the left pane of the DocuSign Signature Appliance Management window and editing the parameters appearing in the right pane. Note that you will

need to perform a Certificate Refresh operation once you finalize the certificate parameter changes (refer to *Refreshing Certificates*).

- ***AIA Publication Location*** – This parameter can be modified. This parameter specifies the publication location of the AIA (Authority Information Access), which contains the DocuSign SA Internal CA certificate.
  This parameter is initially set during DocuSign SA 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 SA 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 DocuSign SA internal CA.
  This parameter is initially set during DocuSign SA 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 SA 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 SA 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 SA 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 validity period*** – Defines the time in years that the end user's certificate is valid.

  Default value: 1 year.

- ***CA Cert Hash Algorithm*** – The hash algorithm used in the certificate generation process by DocuSign SA's internal CA.
  A value of 1 means SHA-1. A value of 2 means SHA-256.
  Default value: 2.
- ***Add Certificate to CRL*** – Specifies whether to add certificates to CRLs when a user is deleted or his/her user data is updated.
  This parameter is also relevant when the DocuSign CA or DocuSign TSCP CA are used.
  Default value: false.
- ***CRL Publishing Frequency*** – How often (in days) the internal CA of DocuSign SA 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.
- ***CPS Object ID*** – You can attach a certificate policy attribute to the certificate generated by the DocuSign SA 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.
- ***Certificate Refresh Window*** – The number of days before the assigned refresh date during which DocuSign SA 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.
  This parameter is also relevant when the DocuSign CA or DocuSign TSCP CA are used. In these cases, it is not recommended to change this value. Please consult with DocuSign support before changing this parameter.
  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 SA 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 SA 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.

- ***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.
  Default value: 31.

  Contact DocuSign support if you wish to modify this value.
- ***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.

  Contact DocuSign support if you wish to modify this value.
- ***CA Key size*** – Read only field showing the key size of the CA.
- ***Certificate's country*** – Country of the CA and user's certificate.
  Note1: In the case of an internal CA, If the user belongs to a group, the country in the certificate is taken from the group.
  Note2: In the case of an internal subordinate CA, the country is determined by the CA.
- ***Certificate's organization*** – Organization of the CA and user's certificate
  Note1: In the case of an internal CA, if the user belongs to a group, the country in the certificate is taken from the group.
  Note2: In the case of an internal subordinate CA, the country is determined by the CA.
- ***Certificate's organizational unit*** – Organizational Unit of the CA and user's certificate
  Note1: In the case of an internal CA, if the user belongs to a group, the country in the certificate is taken from the group.
  Note2: In the case of an internal subordinate CA, the country is determined by the CA.
- ***CA Range*** – The identification of the certificate templates using by the DocuSign CA. This information is entered in the ***Certificate Template*** field upon uploading the RA certificate as described in *Uploading CA Information to DocuSign SA in the case of DocuSign TSCP CA or DocuSign CA*.
  This parameter is relevant when using either DocuSign TSCP CA or DocuSign CA as an external automated CA.
- ***CA Service Connection Point*** – The URL of the DocuSign CA service. This information is entered in the ***CA URL*** filed upon uploading the RA certificate as described in *Uploading CA Information to DocuSign SA in the case of DocuSign TSCP CA or DocuSign CA*.
  This parameter is relevant when using either DocuSign TSCP CA or DocuSign CA as an external automated CA.

- ***Appliance RA Certificate serial number*** – The serial number of the RA certificate that is uploaded to the DocuSign SA as part of the installation of the Appliance or the renewal of the RA key. See *Uploading CA Information to DocuSign SA in the case of DocuSign TSCP CA or DocuSign CA*.
  This parameter is relevant when using either DocuSign TSCP CA or DocuSign CA as an external automated CA.
- ***CA Account Name*** – The identification of the account as it is defined in the Symantec CA Service. This parameter is defined during appliance installation and cannot be modified. This parameter is relevant when using Symantec as the external CA.
- ***CA Service Connection Point*** – The URI of the location where the Symantec CA is located. This parameter is defined during appliance installation and cannot be modified. This parameter is relevant when using Symantec as the external CA.
- ***DocuSign SA Certificate SN*** – The serial number of the authentication certificate used by DocuSign SA to interface with the Symantec CA. This parameter is defined when the PFX file is loaded to DocuSign SA, and cannot be modified. A renewed PFX file has a new SN. This parameter is relevant when using Symantec as the external CA.
- ***External CA User Name*** – The user name representing the organization that enables DocuSign SA to interface with the Comodo CA. This parameter is relevant when using Comodo as the external CA.
  Change this value only in accordance with DocuSign support.
  Default value: as defined during installation.
  This parameter is not relevant anymore.
- ***External CA Password*** – The password corresponding to the *External CA User Name*.
  This parameter is relevant when using Comodo as the external CA
  Change this value only in accordance with DocuSign support.
  Default value: as defined during installation.
  This parameter is not relevant anymore.
- ***The Locality name*** – Determines whether to display the locality field in each generated user certificate. This value is supplied during appliance installation and cannot be modified. This parameter is relevant when using Symantec as the external CA.

Changing DocuSign SA System Parameters

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

To change system parameters:

1. In the left pane of the DocuSign Signature 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 66.

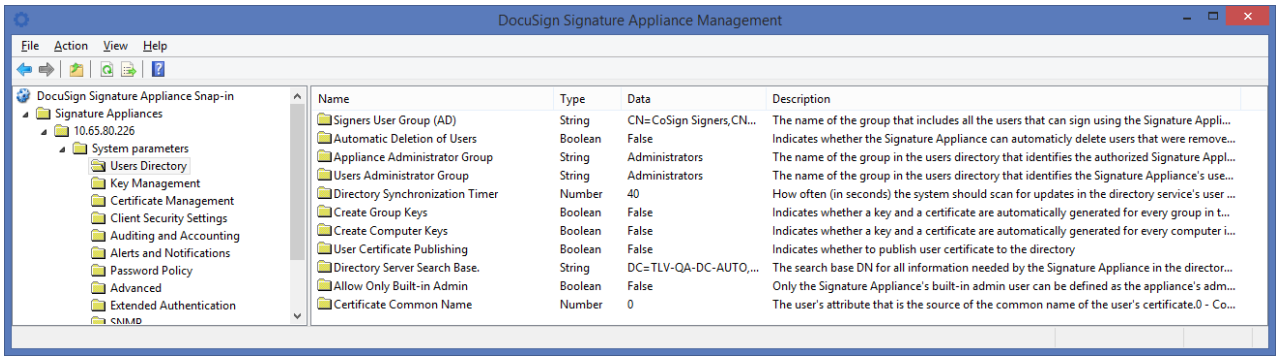


Figure 66 DocuSign SA System Parameters

2. Double-click a parameter to change the parameter's value. A popup dialog box appears with the parameter's current value.
3. 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 DocuSign Signature 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 SA is deployed in a Common Criteria EAL4+ mode of operation.

- ***Signers User Group (AD)*** – The identification of the group in the Active Directory that defines the scope of DocuSign SA users. This group is referred to as the *Signers Group*. This parameter is modifiable and defined during DocuSign SA installation.
  This parameter should be provided in a Full Distinguished Name format, that is, *CN= CoSign Signers, CN = Users, DC= org, 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 SA 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: *DocuSign SA Signers.*
- ***Automatic Deletion of Users*** – If this parameter is TRUE, DocuSign SA automatically deletes a user from DocuSign SA 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= org, DC=com*.

  Default value: administrators.
- ***Users Administrator Group*** – The name of the directory service's user group that identifies authorized DocuSign SA user administrators. Make sure that all users who perform DocuSign SA 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= org, 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 SA synchronization with the directory service, but may decrease DocuSign SA 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 DocuSign SA synchronization with the directory, but may decrease DocuSign SA 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.
  When DocuSign TSCP CA is used, the value of this parameter is True and cannot be modified.

  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.
- ***Allow Only Built-in DocuSign SA 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 SA 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.
- ***Certificate Common Name*** – Defines how to set the value of the common name field in the user certificate. This parameter is relevant only in Active Directory deployments.

  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.

Key Management Parameters

> ***Note:*** This section is not relevant when DocuSign SA 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 SA.

  > ***Note:*** DocuSign SA cannot be configured to extract signature keys.

- ***The Users Key Length*** – The size in bytes of the users' keys. This is relevant if the DocuSign SA 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.
  When DocuSign TSCP CA is used, this value is set to False and it is not recommended to change it.

  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 SA to prepare 200,000 RSA keys in advance.

  This functionality is not supported for cases where DocuSign SA is installed in Common Criteria EAL4+ mode.

  Default value: 0
- ***Key length for RSA Key pool*** – the RSA key length in bytes for the pre-generated RSA key. The values can be either 256, 384 or 512.

  This functionality is not supported for cases where DocuSign SA is installed in Common Criteria EAL4+ mode.

  Default value: 256

Certificate Management Parameters

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

- ***Process Pending Request Timer*** – How often (in seconds) the system should process pending CA-related requests. This parameter is relevant when using DocuSign SA in automatic external CA mode.

  Default value: 60 seconds

- ***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).

- ***Expired user action*** – This parameter is relevant when DocuSign SA is deployed in very large user base scenarios (over 500,000 users). Please contact DocuSign 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 expires.

  Default value: 0.

- ***Delete Expired users by window*** – This parameter is relevant when DocuSign SA is deployed in a very large user base scenario (over 500,000 users). Contact DocuSign 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.

Client Security Setting Parameters

- ***Prompt for Logon*** – Indicates whether the user gets a logon prompt (as shown in *Figure 67*) requiring entry of the user ID, password, and sometime their domain name, when logging on to DocuSign SA.

If set to TRUE, one of the two following dialog boxes appears once, for every user login session in Windows.

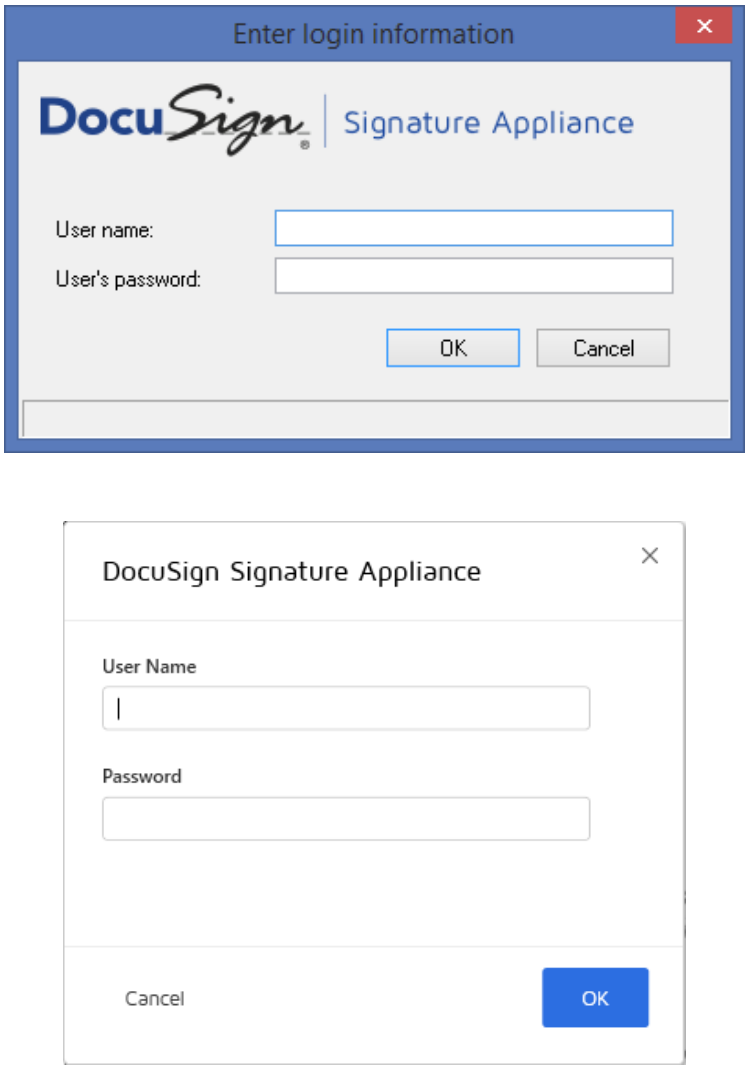


Figure 67 DocuSign SA Logon Prompt

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

***Note**:* In some cases, if no input is entered into any of the logon dialog fields within the first 10 seconds, a 10-seconds 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 DocuSign SA Configuration Utility (refer to the *DocuSign SA Configuration Utility* chapter in the *DocuSign SA User Guide)*.

Default value: False.

- ***Prompt for Signature*** – Indicates whether the user gets a prompt (as shown in *Figure 67*) requiring entry of the user's password before each digital-signature creation.

  When using extended authentication, this parameter must be set to True.

  When DocuSign TSCP CA is used, this parameter is set to True and cannot be changed.

  When DocuSign CA is used, this parameter is set to True by default.

  If SAML/JWT based authentication is used, it is possible to pass a SAML/JWT token as a password. In this way, it will be possible to continue with the signature operation if this parameter is 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.
  When the Appliance is installed in Common Criteria mode the value is False and cannot be changed.

  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 DocuSign 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 audit 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 audit 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 DocuSign Signature Appliance audit log.
  Default value: 7
- ***Maximum number of rows*** – Indicates the maximum number of rows permitted in the auditing table. When the specified amount is reached, the oldest entries are deleted.
  Default value: 30,000

Alerts and Notifications Parameters

- ***Mail Server Name*** – DNS name or IP address of the SMTP server used for sending email notifications.
  This parameter is not used when the Appliance installed in Common Criteria mode.
  Default value: No mail server
- ***Mail Server Port*** – The TCP/IP port number of the SMTP server used for sending email notifications.
  This parameter is not used when the Appliance installed in Common Criteria mode.
  Default value: 25.
- ***Email From Address*** – The source email address to be used for sending email notifications.
  This parameter is not used when the Appliance installed in Common Criteria mode.
  Default value: none.
- ***Syslog Server IP Address*** – The IP address of the syslog server. If the proper IP is set, some events are reported to the syslog server.
  Starting from DocuSign SA version 9.3, a large number of syslog events were added to the system. Many of the audit log events that are written to the audit log are also sent out 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 SA user. The minimal length cannot be set to less than 6 characters.

When the Appliance is deployed in Common Criteria mode the Minimum Password Length must be set to no less than 8 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 SA 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 SA 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 SA 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 SA 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 DocuSign SA 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 DocuSign SA 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.

  If LDAP is used to access Microsoft Active Directory, this parameter should be set with the *User-Principal-Name* value. If you choose to use the *sAMAccountName* value instead, this may cause a problem when authenticating using a SAML ticket.

  Consult with DocuSign 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 DocuSign support.

- ***Appliance Debug Level*** – Modify this parameter only when instructed to do so by DocuSign's technical support team.

> ***Note:*** Running in debug mode (i.e., DocuSign SA Debug Level is greater than 2) significantly decreases DocuSign SA performance levels.

Default value: 2.

- ***Clients Inactivity Timeout*** – The time period after which DocuSign SA disconnects inactive clients, in seconds.

  > ***Note:*** In environments with thousands of DocuSign SA clients, it is recommended to decrease this value to several minutes. This reduces usage of appliance resources by DocuSign SA 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 an External CA in automated mode to get users' certificates.
  This parameter is not used when the Appliance installed in Common Criteria mode.

  Default value: false.

- ***SSL Proxy IP*** – If DocuSign SA is installed in an organization which allows access to the internet only through an HTTP proxy, DocuSign SA 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.
  This parameter is not used when the Appliance installed in Common Criteria mode.

  Default value: empty.

- ***SSL Proxy Port*** – If DocuSign SA is installed in an organization which allows access to the internet only through an HTTP proxy, DocuSign SA 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.

  This parameter is not used when the Appliance installed in Common Criteria mode.

  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.
  This parameter is not used when the Appliance installed in Common Criteria mode.

  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.
This parameter is not used when the Appliance installed in Common Criteria mode.

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 DocuSign SA 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 DocuSign SA REST API.
  In these cases, this system parameter can be set to enable interacting with the DocuSign SA 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 SA to operate in FIPS mode. When DocuSign SA 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. 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.

  Note: When DocuSign SA is installed in Common Criteria EAL4+ mode, this parameter shall not be changed and shall have the default value of 0.0.0.0

- ***Common Criteria Mode*** – This parameter indicates whether DocuSign SA is installed in Common Criteria EAL4+ mode. If it is, the parameter has a value of True.
- ***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 – Should not be used by customers
  - 2 – External Production-based cloud monitoring. Should be used when the appliance is deployed by customers.
  - 3 – Should not be used by customers

  Default value: 0
- ***Cloud Site ID***– a string identification value that should be configured if instructed to do so by DocuSign Support.

  Default value: empty
- ***Minimum server TLS version*** – This parameter indicates the TLS version.
  It can have one of the following values:
  - 0 – TLS versions 1.0, 1.1 and 1.2 are allowed
  - 1 – TLS versions 1.1 and 1.2 are allowed
  - 2 – Only TLS version 1.2 can be used

  When the Appliance is deployed in Common Criteria EAL4+ mode, the value of this parameter must be set to 2 (that is, TLS version 1.2 only).

  Default value: 0

  Note: It is also possible to configure the Appliance to allow the TLS to use only AES based mechanisms. Refer to *Disable 3DES in TLS*.
- ***Disable 3DES in TLS*** – If this parameter is set to True, only AES-based security mechanisms will be used as part of the regular TLS communication between clients and the Appliance.

  When the Appliance is deployed in Common Criteria EAL4+ mode, this parameter must be set to True.

  Default value: False
- ***Common Criteria Type*** – This parameter indicates the type of Common Criteria EAL4+ mode. It can have one of the following values:
  - 0 – DocuSign SA is installed as a Signature Creation Device
  - 1 – DocuSign SA is installed as a Seal Creation Device

  This value cannot be changed after the appliance is installed.
- ***Cloud Monitoring Reporting Type*** – The type of additional information sent to the DocuSign monitoring system.
  This field receives a bit flag value, meaning that you can set a combination of parameters. Contact DocuSign Support for more information.
  - 1 – Basic

- 2 – Marketing
- 4 – Support.
- 8 – Licensing

Default value: 1

- ***Cloud Monitoring timer*** – The reporting time interval (in seconds)
  Default value: 86400 seconds.
- ***HSM Mode*** – Is set to true if the Appliance is deployed in HSM mode.
  Default value when Signature Appliance is deployed: false.

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.
  When the Signature Appliance is deployed in CC EAL4+ mode, the Signature Appliance interacts with the external Radius Server, however, the actual OTP validation is performed by the Signature Appliance.
  The parameters described in *Extended Authentication – Radius* enable DocuSign SA to communicate with the Radius Server.
- ***One Time Password using an internal OTP mechanism*** – The end user enters a One Time Password (OTP) using a special device. The One Time Password is internally validated by the DocuSign Signature Appliance.
  The parameters described in *Internal OATH TOTP* are used when the internal OTP is used for extended authentication.

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 SA uses the regular password verification mechanism.
  1 – Radius based extended authentication.
  2 – SmartCard based extended authentication – Not Applicable.
  3 – Biometric based extended authentication – Not Applicable.
  4 – Internal OATH TOTP: internal OTP mechanism is used.

  When DocuSign SA is installed in Common Criteria EAL4+ mode as a Qualified Signature Creation Device, the value can be either 1 or 4, and not anything else.

  Default: 0.

  Alternate Extended Auth mode –This parameter is deprecated.

Extended Authentication – Biometric –Deprecated

Extended Authentication – SmartCard – Deprecated

Extended Authentication – Radius

- ***Require Static Password*** – When this value is true, the end user must enter DocuSign SA's 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 SA 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 SA will authenticate the user using the DocuSign SA 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 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.
- ***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 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 SA 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 SA 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:
  - 0 – Disabled
  - 1 – CC OATH-HOTP – a standard OATH-based OTP device that is an event based OTP. This mode can be used when the Signature Appliance is deployed in CC EAL4+ mode when a Radius Server is deployed.
  - 2 – Internal OATH TOTP – a standard OATH-based OTP device that is a time-based OTP. This mode is used when no Radius Server is deployed (in either CC EAL4+ mode or in a regular deployment).
  - 3 – VASCO – An OTP devices manufactured by Vasco. This mode can be used when the Signature Appliance is deployed in CC EAL4+ mode when a Radius Server is deployed.
- ***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.
  The maximum allowed value for the Sign Window is 600 seconds (10 minutes).

  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 DocuSign SA SNMP service is on or off.

  If the DocuSign SA SNMP Service is on, the DocuSign Signature Appliance can be used

by a monitoring server to inspect information.
The MIB identity of the DocuSign SA software is **1.3.6.1.4.1.2774.3.1,** where the prefix **1.3.6.1.4.1.2774** specifies DocuSign as the vendor of the DocuSign Signature Appliance product.

Default: False.

- ***SNMP Accepted community name –*** Defines which community members can manage the DocuSign SA's 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 SA and present an SAML ticket provided by a trusted organizational server.

> ***Note:*** The following SAML parameters are not relevant when DocuSign SA 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 DocuSign SA Service and in subsequent login operations.
  - 2 – User with group association – Only users who are associated with a DocuSign SA group can present an SAML token as part of their initial connection to the DocuSign SA Service and in subsequent login operations.
- ***Accept Relying Parties Tickets*** – The name of the DocuSign SA Service as identified by the relying parties that generate the SAML tickets. The DocuSign SA 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 SA, the SAML group name must match an existing group defined in the DocuSign Signature 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.
- ***SAML Object Guid*** – the name of the attribute in the SAML ticket that stores the GUID of the Object.
  Default: objectGuid.
- ***SAML Groups Member*** – the name of the attribute in the SAML ticket that stores the groups member.
  Default: groupsMember.
- ***SAML Fetch Additional User Info*** – If the DocuSign SA is installed in Active Directory mode or LDAP mode, and this parameter is set to True and in addition the user does not exist in the DocuSign SA's database, user existence will be checked in the domain.
  In cases where the DocuSign SA is installed in Active Directory mode and the DocuSign Signature Appliance is synchronized with users belonging to an Active Directory group, user's membership in the Active Directory group will be checked, even if this value is set to False.
  Default: False.
- ***SAML Ignore Revocation Status*** – Specifies whether to ignore the revocation status of the certificate that created the SAML token. This is mainly relevant for deployments where the Signature Appliance will have a problem in connecting for the purpose of fetching the CRL that matches the certificate of the SAML token.
  Default: False.

JWT

You can connect to DocuSign SA and present a JWT ticket provided by a trusted organizational server.

Note: The following JWT parameters are not relevant when DocuSign SA is installed in Common Criteria EAL4+ mode.

- **JWT *Working Method*** – The JWT authentication mode used for Logon operation. The possible values include:
  - 0 – Disabled – It is not possible to present a JWT token as part of the user login process.
  - 1 – All Users – All users can present a JWT token as part of their initial connection to the DocuSign SA Service and in subsequent login operations.
- ***OpenID Discovery Document*** – This URL can be used to access the identity provider for receiving information that is relevant to the validation process of the JWT token. If this URL is not supplied, the values of *JWT Issuer* and ***JWT Set Document*** are used.
- ***JWT Issuer*** – The name of the Issuer of the tokens. This value is mandatory if the *OpenID Discovery Document* parameter is not defined.
- ***JWT Audience*** – the expected audience of the JWT token. If this value is specified, only the JWT Audience that matches the specified audience will be accepted.
- ***JWT Set Document*** – This URL is mandatory if the *OpenID Discovery Document* parameter is not defined. Using this URL, the DocuSign SA will access the Identity Provider to get information that enables validating the JWT ticket.
- ***JWT Symmetric Key*** – if the JWT ticket validation scheme is symmetric (that is, based on an HMAC algorithm), this parameter will include the JWT Symmetric Key.
- ***JWT Common Name*** – The name of the attribute in the JWT ticket that stores the end user's common name.

  Default: name
- ***JWT Email Address*** – The name of the attribute in the JWT ticket that stores the end user's email address.

  Default: email.
- **JWT *UPN*** – The name of the attribute in the JWT ticket that stores the end user's identity.
- **JWT *Telephone Number*** – The name of the attribute in the JWT ticket that stores the end user's telephone number.
- **JWT *Display Name*** – The name of the attribute in the JWT ticket that stores the end user's Display Name.

  Default: displayName.
- **JWT *Group Name*** – The name of the attribute in the JWT ticket that stands for the end user's Group. In order to utilize the Group functionality of DocuSign SA, the JWT group name must match an existing group defined in the DocuSign Signature Appliance.
- **JWT *Object Guid*** – the name of the attribute in the JWT ticket that stores the GUID of the Object.

- **JWT *Groups Member*** – the name of the attribute in JWT ticket that stores the groups member.
- **JWT *Window*** – The grace period in minutes during which the JWT ticket is still valid beyond the formal expiration time of the JWT ticket, as well as the time period in minutes that the JWT ticket is valid before the formal starting time of the JWT ticket.
  This parameter is intended to solve time synchronization issues.
  Default: 5 minutes.
- **JWT *Fetch Additional User Info*** – If the DocuSign SA is installed in Active Directory mode or LDAP mode, and this parameter is set to True and in addition the user does not exist in the DocuSign SA's database, user existence will be checked in the domain.
  In cases where both Active Directory mode and group license mode are implemented, user existence will be checked in the group license even if this value is set to False.
  Default: False.

Internal OATH TOTP

The following configuration parameters are used when the internal OTP is used for extended authentication. The internal OTP mechanism is based on the OATH-TOTP standard.
This mode can be used when the signature Appliance is deployed in CC EAL4+ mode.

- ***OTP Validity period*** – The time, in seconds, that the presented OTP is valid.
  Default: 30 seconds
- ***OTP length*** – The number of digits of the OTP (One Time Password)
  Default: 6 digits
- ***Internal OTP enabled*** – This read only parameter's value is True if the value of *Extended Authentication Method* is 4; otherwise, its value is False.
- ***Time to init OTP after reset*** – the amount of time in minutes given to the user to download the shared secret after the administrator gave the user permission to get his/her shared secret.
  Default: 1440 minutes – meaning one day

Restoring the DocuSign Signature Appliance

The Restore operation enables you to restore the DocuSign Signature Appliance from a previously generated backup file (refer to *Backing up the DocuSign SA Data*). You may wish to do this if there has been data loss or corruption or if you want to set up a new DocuSign Signature Appliance with the data from a previously installed appliance.

The Restore operation is similar to installation (refer to *Installing the DocuSign Signature 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.

***Note**:* This operation is not relevant when the appliance is deployed to use a DocuSign TSCP CA.

Restoring the DocuSign Signature Appliance in Microsoft Active Directory

Note: In order to run the restore operation, you must have permissions similar to those required for installing the DocuSign Signature Appliance software. Refer to *Installing the DocuSign Signature Appliance Software* for more information.

To restore the DocuSign Signature Appliance:

1. Make sure the appliance is in Factory Settings mode. You can check whether the **Install** state is **Factory** in the consoles' **Status** tab (refer to *Displaying DocuSign Signature Appliance Status*). To restore DocuSign SA to its factory settings, refer to *Restoring Factory Settings*.
2. In the *DocuSign Signature Appliance Management* window (*Figure 54*), right-click **DocuSign Signature Appliances** and select **All Tasks** → **Restore** from the popup menu. A standard file selection dialog box appears.
3. Browse to the backup file, and click **Open**.
4. Enter the IP address of the DocuSign Signature Appliance and click **Next**. The *User setup* dialog box appears.
5. Click **Next**. Enter the built-in DocuSign SA administrative user. You must provide the password of the built-in administrative user and confirm the password.
6. Enter the **Admin user name** and **Admin password** of an administrator who has p**ermission to join the DocuSign Signature Appliance to the domain**.

   Note: The **Admin user name** enables DocuSign SA to register computers as members of the domain during restoration. DocuSign SA 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.
7. Click **Next**. DocuSign SA restoration begins. A status bar displays the status of the restore operation.
8. At the prompt, insert the backup MiniKey token that was used when first installing this appliance. DocuSign SA reads the data from the MiniKey token. No writing to the MiniKey token is performed at this stage.
9. At the prompt, insert the license MiniKey token.

When the operation is complete, the message `Installation of DocuSign Signature Appliance finished successfully` appears above the status bar.

Note: It is highly recommended to restart the DocuSign Signature Appliance and synchronize DocuSign SA with the Active Directory immediately after restoring the DocuSign Signature Appliance. For more information, refer to *Synchronizing DocuSign SA with the Directory Service*.

Restoring the DocuSign Signature Appliance in an LDAP Environment

To restore the DocuSign Signature Appliance:

1. Make sure the appliance is in Factory Settings mode. You can check whether the **Install** state is **Factory** in the consoles' **Status** tab (refer to *Displaying DocuSign Signature Appliance Status*). To restore DocuSign SA to its factory settings, refer to *Restoring Factory Settings*.
2. In the *DocuSign Signature Appliance Management* window (*Figure 54*), right-click **DocuSign Signature Appliances** and select **All Tasks** → **Restore** from the popup menu. A standard file selection dialog box appears.
3. Browse to the backup file and click **Next**.
4. Enter the IP address of the DocuSign Signature Appliance.
5. Click **Next**. Enter the built-in DocuSign SA 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.
6. Click **Next**. DocuSign SA restoration begins. A status bar displays the status of the restore operation.
7. At the prompt, insert the backup MiniKey token that was used when first installing this appliance. DocuSign SA reads the data from the MiniKey token. No writing to the MiniKey token is performed at this stage.
8. At the prompt, insert the license MiniKey token.

When the operation is complete, the message `Installation of DocuSign Signature Appliance finished successfully` appears above the status bar.

Restoring the DocuSign Signature Appliance in a Directory Independent Environment

To restore the DocuSign Signature Appliance:

1. Make sure the appliance is in Factory Settings mode. You can check whether the **Install** state is **Factory** in the consoles' **Status** tab (refer to *Displaying DocuSign Signature Appliance Status*). To restore DocuSign SA to its factory settings, refer to *Restoring Factory Settings*.

2. In the *DocuSign Signature Appliance Management* window (*Figure 54*), right-click **DocuSign Signature Appliances** and select **All Tasks** → **Restore** from the popup menu. A standard file selection dialog box appears.
3. Browse to the backup file and click **Next**.
4. Enter the IP address of the DocuSign Signature Appliance and click **Next**. The *User setup* dialog box appears.
5. Click **Next**. Enter the built-in DocuSign SA administrative user. You must provide the password of the built-in administrative user and confirm the password.

   Note: If you perform a restore in a Common Criteria environment, make sure that the entered built-in user administrator user is not defined in the system's backup as a non-user administrator. This will lead to an error in the restoration process.
   If you have any doubt, create a new user administrator that was never used before.

   In the following pages, default settings from the original installation will appear disabled. Click **Next** at every page.
6. Click **Next**. DocuSign SA restoration begins. A status bar displays the status of the restore operation
7. At the prompt, insert the backup MiniKey token that was used when first installing this appliance. DocuSign SA reads the data from the MiniKey token. No writing to the MiniKey token is performed at this stage.
8. At the prompt, insert the license MiniKey token.

When the operation is complete, the message `Installation of DocuSign Signature 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 SA is installed in a Directory Independent environment as well as the ability to view and perform some actions upon users when DocuSign SA 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 SA is installed in Common Criteria EAL4+ mode.
- Enable a user to log in to DocuSign SA or disable a user from logging in to DocuSign SA.
- View users' information.
- Reset global and user-based signature counters.
- Unlock a user after several consecutive authentication failures.
- Enable a user to download the OTP shared secret when the internal OTP mechanism is used.

- Revoke a user's certificate if DocuSign TSCP CA or DocuSign CA is used,

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 SA.
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 SA groups by assigning each user to a group after the user is copied from the Active Directory to DocuSign SA.

When SAML/JWT with Directory Independent deployment is used, a user that initially connects to the DocuSign Signature Appliance by presenting a SAML/JWT ticket is automatically assigned to a group if the SAML/JWT ticket contains a Group attribute.

Group management is not enabled when DocuSign SA 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 SAPI. For more information on the DocuSign SAPI, refer to the *DocuSign SA Signature APIs Developer's Guide*.

> ***Note****:* If the DocuSign SA REST interface will be used, you must make sure that the User Logon is based only on alphanumerical characters and the following characters: _ or - (underscore or hyphen). Any other characters such as /\ cannot be used.

Activating the Users Management Utility

The `Users Management` utility is installed as part of the `DocuSign Signature Appliance Admin` client component.

To activate the `Users Management` utility:

1. In the system tray, right-click the  icon and select **Administrative Tools → Users Management**.

   The `Users Management` main window appears.

2. Use the **Login** or **Login built-in user** option to enable the administrator to login to DocuSign SA.

3. 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 SA 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.

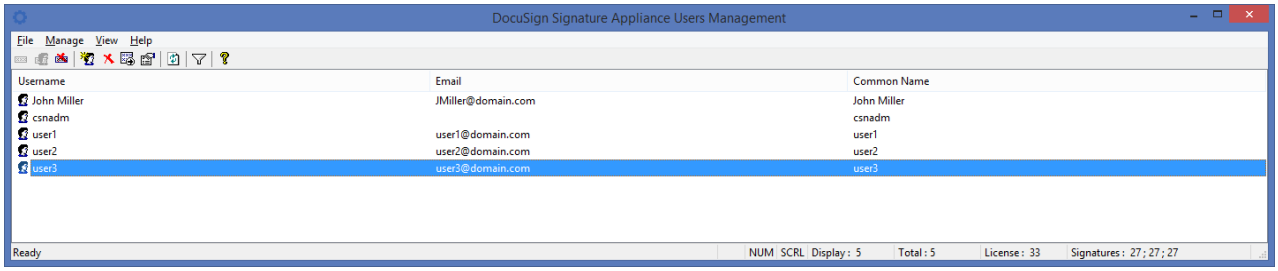


Figure 68 Directory Independent Users Management Utility - Main Window

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 SA 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 SA 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 SA.

- **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** – Not Applicable. Please ignore this value.
- **Enrollment reason** – Not Applicable. Please ignore this value.

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 SA 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 SA since the counter was last reset.

Generate Users report

Enables generating a report for all DocuSign SA users. This report contains all the important DocuSign SA 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 SA. The administrator is prompted for his/her user ID and password. If DocuSign SA 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 SA.

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 SA operates in a Directory Independent environment. This option enables adding a new user to DocuSign SA. When this option is selected, the *New User* dialog box appears.

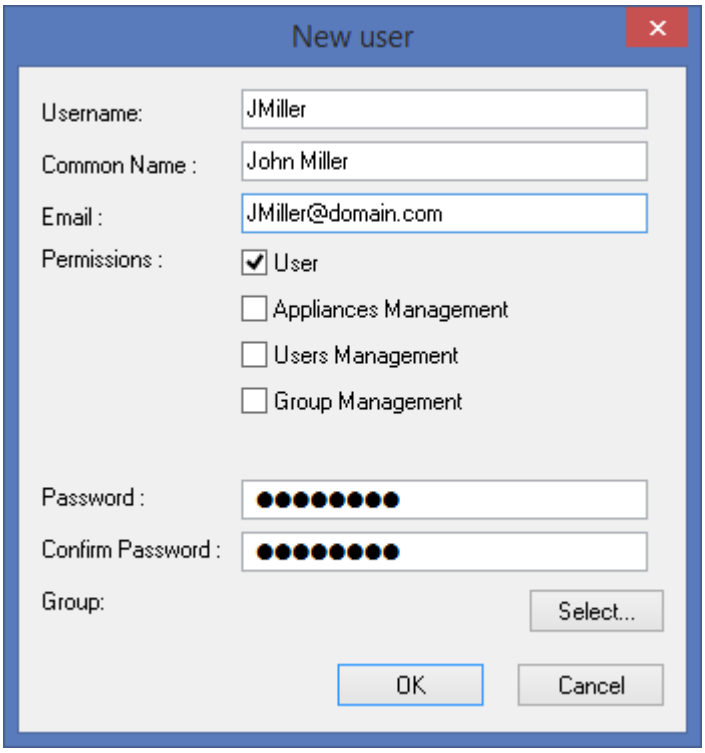


Figure 69 Users Management Utility – New User Dialog Box

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.

  If an external automated CA is used, it is mandatory to enter an email for the user, otherwise the external CA will not be able to issue a certificate for the user.
- **Permissions** – The user's authorizations. Select one or more of the following:
  - **User** – A regular DocuSign SA user.
  - **Appliances Management** – Permission to perform administrator activities, such as downloading the audit log and backing up the database.
  - **Users Management** – Permission to manage DocuSign SA users.
  - **Group Management –** Permission to manage users in the group to which this user belongs.
  - When DocuSign SA 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.

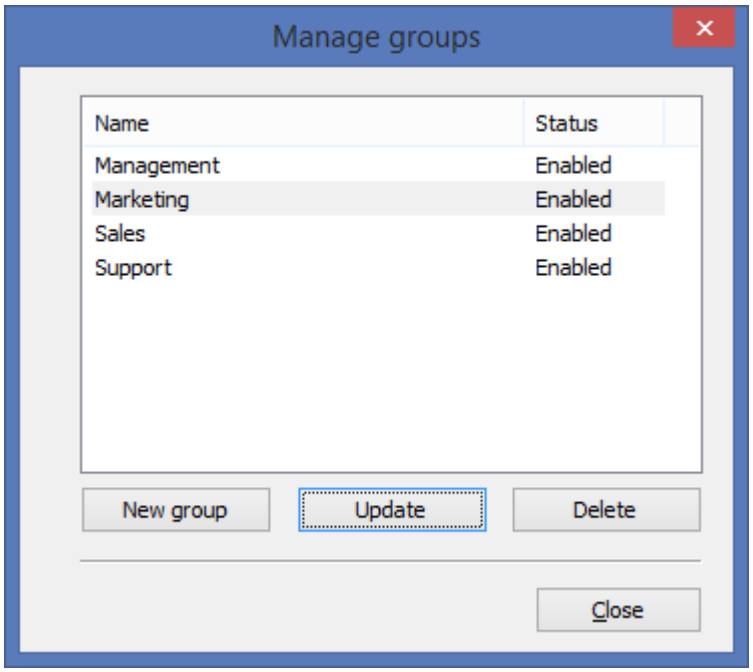


Figure 70 Manage Groups Dialog Box

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 SA 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.

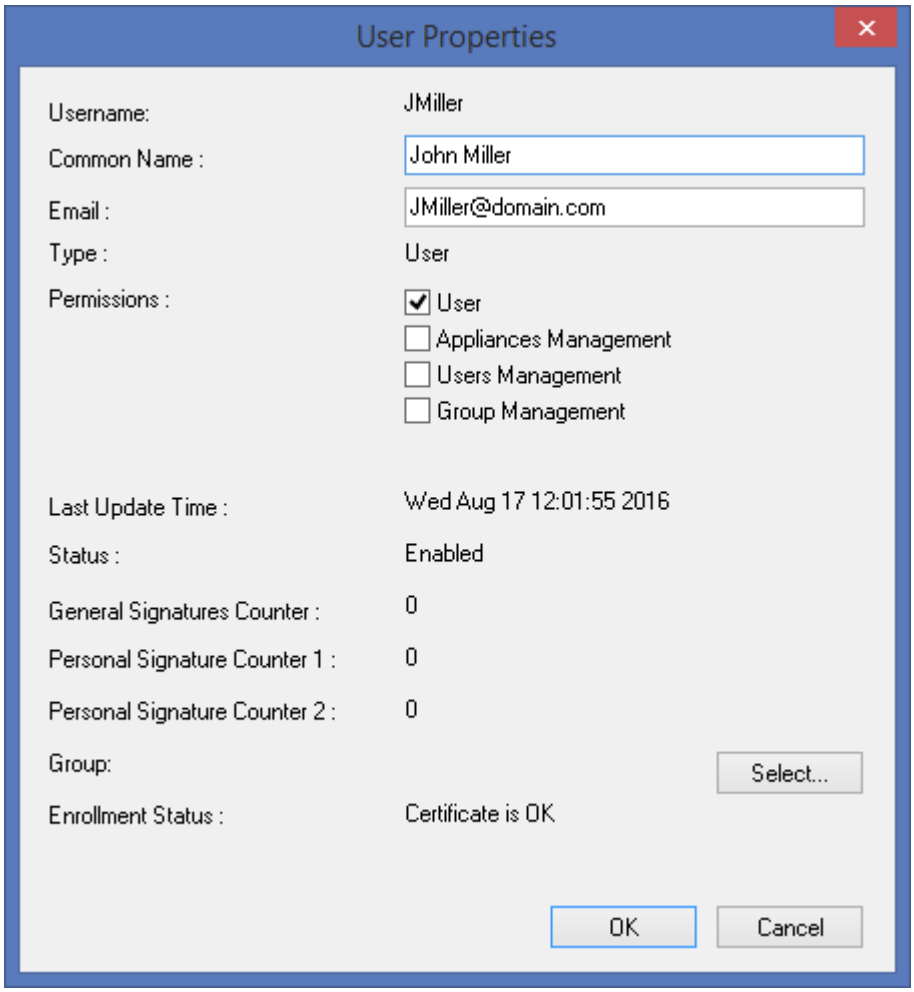


Figure 71 Users Management Utility – User Data Dialog Box

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 SA 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 SA.

The dialog box lists all existing groups inside DocuSign SA and their status (Enabled or Disabled). When a group is Disabled, all users who are members of the group cannot login to DocuSign SA.

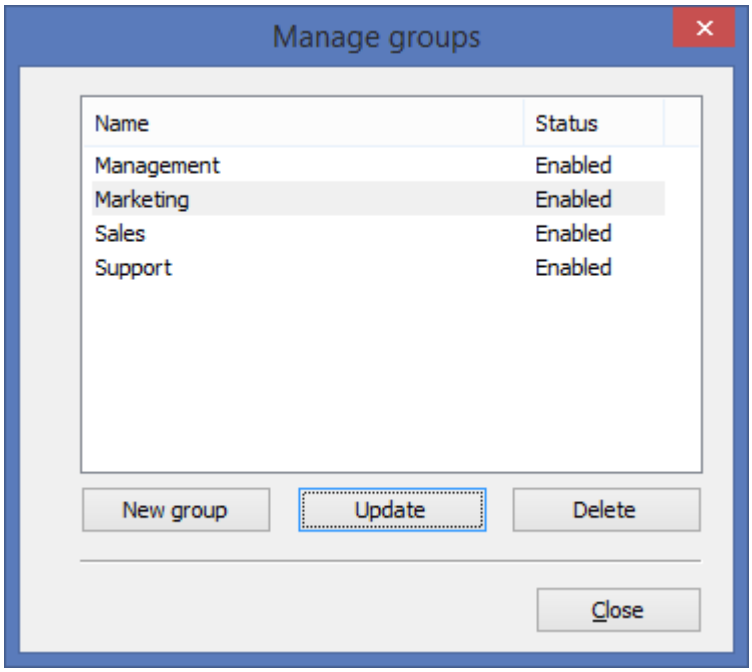


Figure 72 Users Management Utility – Manage Groups Dialog Box

You can perform the following operations:

- **New Group** – Add a new group to DocuSign SA. When you click **New Group**, the *Group Settings* dialog box appears:

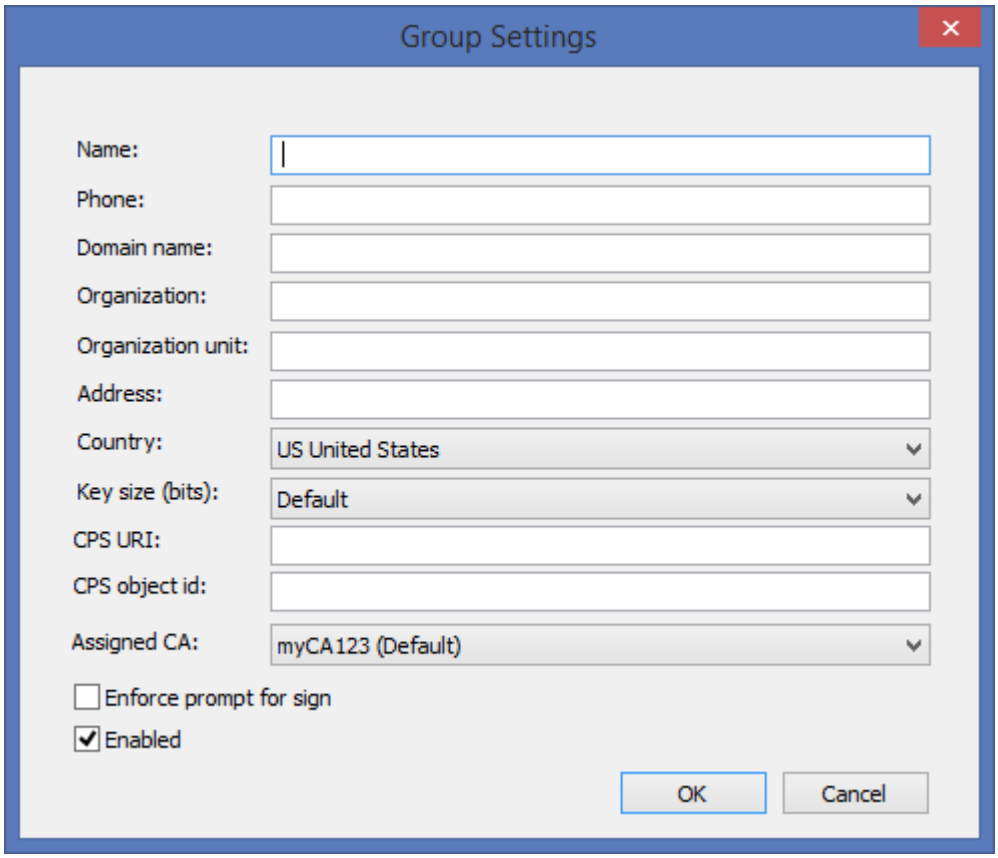


Figure 73 Users Management Utility – Group Settings Dialog Box

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. This parameter was removed in DocuSign SA version 8.5.
- **Assigned CA –** Starting from DocuSign SA version 8.5, it is possible to assign a group to a specific CA, with the result that all users belonging to the group will get their certificates from the assigned CA. The above certificate-related parameters will apply to the certificate that is generated for the users that belong to this group.
- **Enforce prompt for sign** – If the system parameter **Prompt For Sign**ature 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 SA.

- **Update** – Update the selected group. When you click **Update**, the *Group Settings* dialog box appears (Figure 73), 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 73). You can view and modify any of the settings.

New Group

Note: This operation is not relevant when DocuSign SA 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 73) appears. For explanations, refer to the explanations following Figure 73.

Revoke Certificate

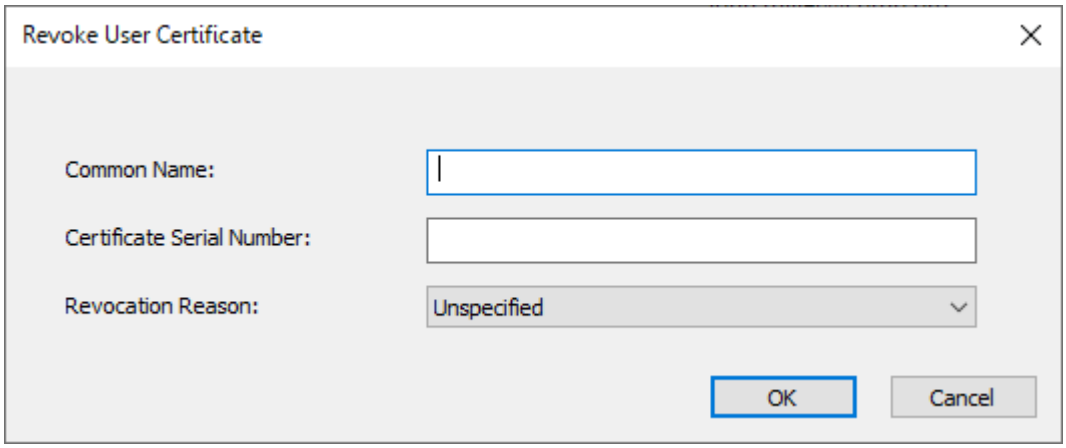
Note: This operation is relevant only when DocuSign SA is configured to use DocuSign CA and DocuSign TSCP CA.

Note:When the DocuSign Signature Appliance is deployed in AD environment, please have the user removed from the signers group prior to revocation.
When the DocuSign Signature Appliance is deployed in DI environment, please have the use deleted after performing the revocation operation.

.

Revokes a user's certificate by notifying the DocuSign CA or DocuSign TSCP CA.

In the *Revoke User Certificate* dialog box that appears, specify the **Certificate Serial Number** of the certificate being revoked, and select the **Revocation Reason** from the list. It is not required to fill in the **Common Name**.



Note: In the case that you sent a revocation for a user and you either get an error or you suspect that the revocation command did not reach DocuSign CA or DocuSign TSCP CA.
Please repeat the operation by entering the certificate serial number.

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.

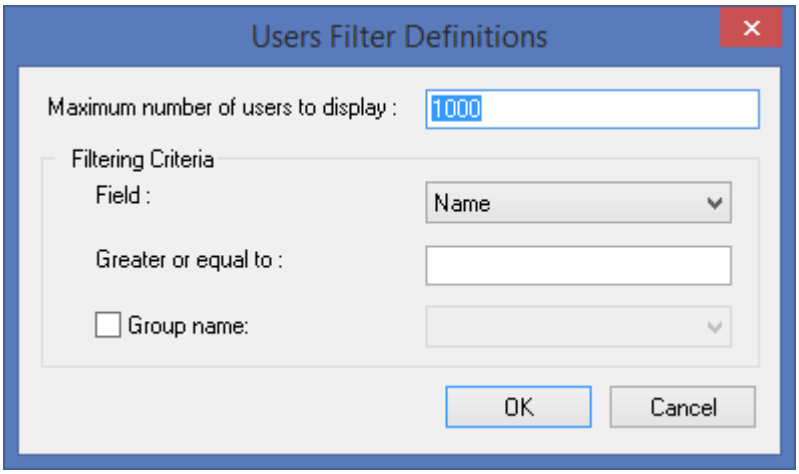


Figure 74 Users Management Utility – Users Filter Definitions Dialog Box

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: 1000.
- **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.

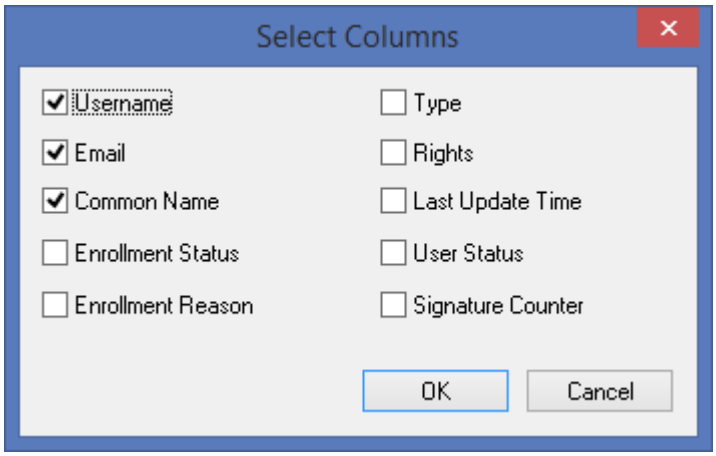


Figure 75 Users Management Utility – Select Columns Dialog Box

Help

Displays the About window that specifies the `Users Management` version and provides a link to the DocuSign 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
	Revoke User

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**, **Enable user to export secret**, **Delete**, **Set Password**, **Properties**, **Assign Group** (included in **New**) and **Revoke User** 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, Enable user to export secret**, **Assign Group** and **Revoke User** options are described below.

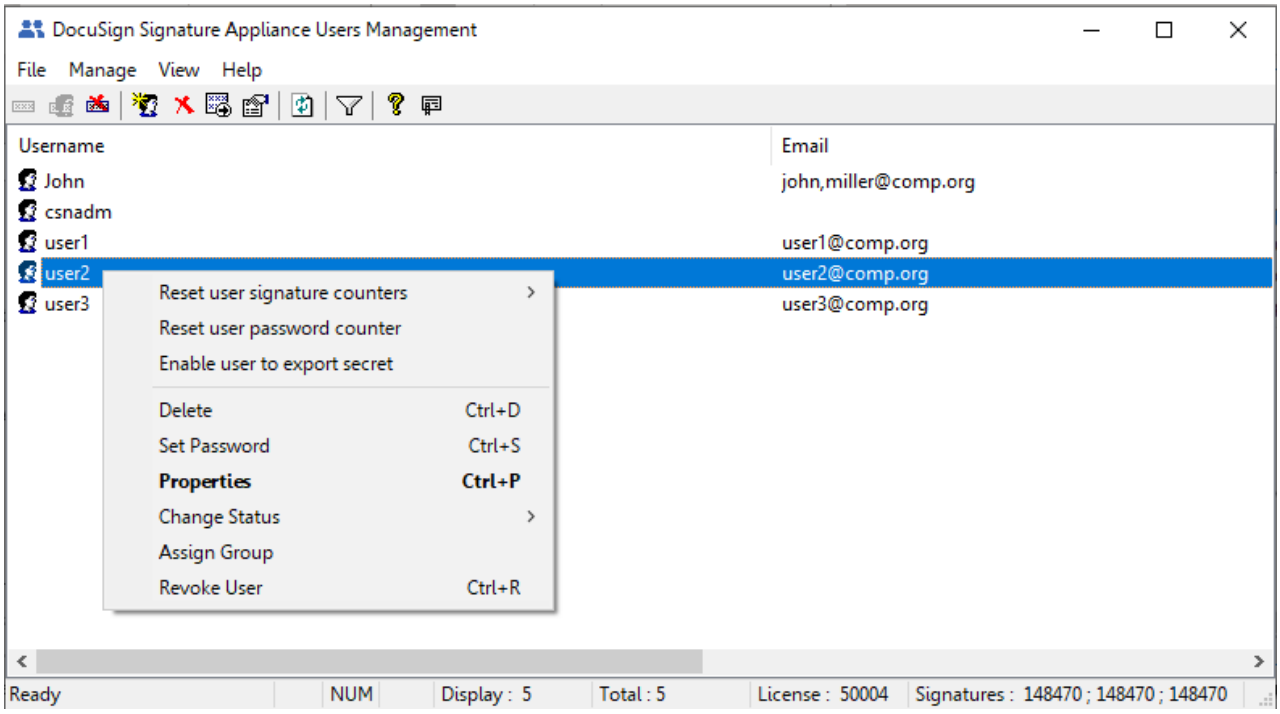


Figure 76 Users Management Utility – Right-click Menu

Enable user to export secret

To enable the user to securely download his/her OTP shared secret, the user administrator must select this option. The user is then granted a certain amount of time to connect to the Signature Appliance for downloading the shared secret.
This operation is applicable only when the Signature Appliance is configured to work with an internal OTP.
When the Signature Appliance is deployed in CC EAL4+ mode, the shared secret can only be downloaded prior to Account Activation.

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.

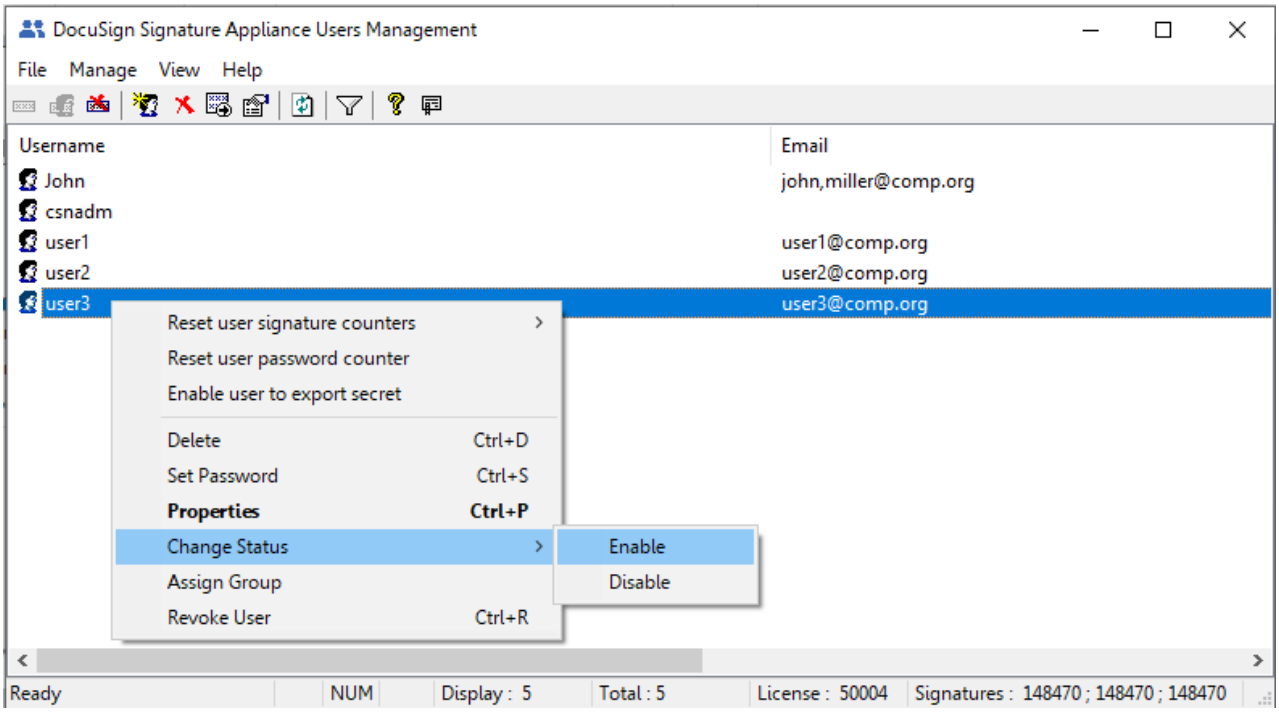


Figure 77 Users Management Utility – Change Status Option

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 70), with options for assigning/unassigning a user.

Revoke User

This option can be used when the DocuSign SA is connected to a DocuSign TSCP CA or DocuSign CA. This option should be used for notifying the CA of a user certificate that needs to be revoked.
In the *Revoke User Certficate* dialog box that appears you need to specify the **Revocation Reason**.

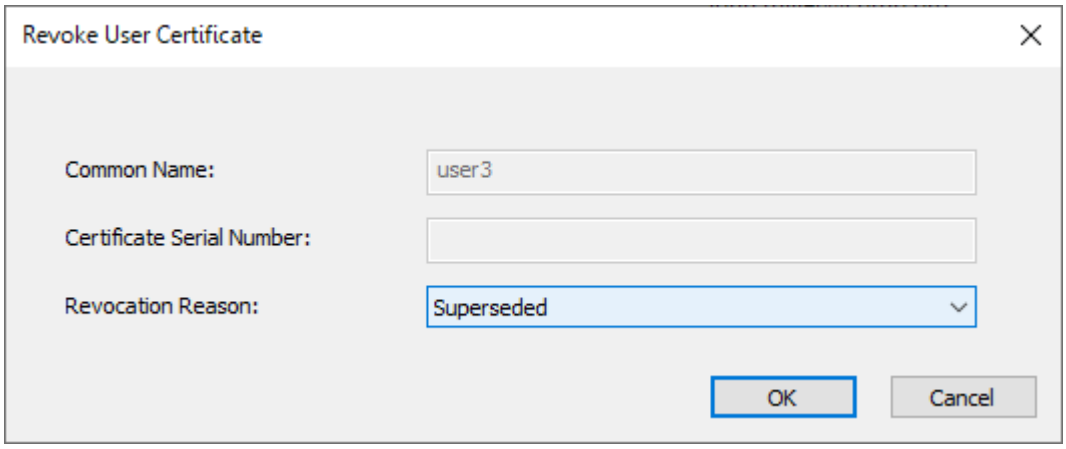


Figure 78 Users Management Utility – Revoke User Certficate Option

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 DocuSign Signature Appliance.
- `GetEvt` – Retrieves the audit log of the DocuSign Signature Appliance.
- `SetSCP` – Sets the working state of the DocuSign Signature Appliance.
- `RestartServer.exe` – Restarts a DocuSign SA Server.
- `Switch2Prim.exe` – Performs a Switch-to-Prime operation for a given alternate appliance.
- `getServerReport.exe` – Generates a report listing the number of users and number of digital signatures produced by the Appliances in the cluster.
- `AuditLogDownloadUtility.exe` – Downloads audit logs from both the primary appliance and the alternate appliances.

All these utilities are installed as part of the `DocuSign Signature Appliance Admin` component and located under `Program files (86)\ARX\ARX CoSign Admin Client`, when the client is deployed in a 64bit Windows OS.

> ***Note:*** To display the required parameters for a command, execute the command without any parameters. In the case of the `AuditLogDownloadUtility.exe` utility, you need to supply the `/?` parameter.

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 DocuSign SA Administration MMC (refer to *Backing up the DocuSign SA Data*).

The following table describes the available parameters for `GetBackup`:

Parameter	Description
`-F <Output File name>`	Output file name of the backup file.
`-IP <IP Address>`	IP address of the DocuSign Signature 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 <DocuSign SA 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 SA administrator user name.
`-P <User Password>`	Password of the DocuSign SA administrator user.
`-D <Domain Name>`	Name of the domain or context.

GetEvt

The `GetEvt` command enables you to retrieve the compressed audit log from the DocuSign Signature Appliance.

Note: This command provides the same functionality as the **All Tasks → Download Logs → Signature Appliance Audit Log** option in the DocuSign SA Administration MMC (refer to *Downloading Log Files*).

The following table describes the available parameters for `GetEvt`:

Parameter	Description
`-F <Output File name in zip format>`	Output file name of the zipped audit log file.
`-IP <IP Address>`	IP address of the DocuSign Signature Appliance. If this value is omitted, it will be taken from the SCP or from the client configuration.

Parameter	Description
`-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 <DocuSign SA 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 SA administrator user name.
`-P <User Password>`	Password of the DocuSign SA administrator user.
`-D <Domain Name>`	Name of the domain or context.

restartServer.exe

The `restartServer.exe` utility restarts a DocuSign SA 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 DocuSign Signature Appliance 2 - Shut down the DocuSign Signature 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. 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 SA 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
`-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 SA 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. This is the name of the DocuSign SA 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. Possible values: ☐ `Up` ☐ `Down`

getServerReport

This utility produces a report listing the number of users in the system and the number of digital signature operations made with the system.

The utility requires administrative credentials for producing a proper report.

The report issue the following figures for every Appliance in the cluster:

- Number of Users – The actual number of users in the Appliance database. This value should be the same for every Appliance in the cluster.
- Current period transaction counter – The number of digital signatures created during the current license period.
- Total signatures counter – The total number of digital signatures made by this appliance.

The report also includes a summary of information gathered from all appliances where the *Current period transaction* counter and *Total signatures counter* are a summation of the individual cluster appliances counters.

AuditLogDownloadUtility.exe

This utility should be used when DocuSign TSCP CA is used. In this configuration it is mandatory to download all audit logs from the appliance(s) to the administrative client and archive them for 10.5 years.
This utility should be used to download audit logs from both the primary appliance and the alternate appliances when applicable.

This tool performs the following:

1. Downloads the exising audit log from the appliance.
2. The downloaded audit log is signed by the administrator.
   This means that the administrator must be a signer in the system.
   The administratoir will be prompt with to enter his/her password.
   When the appliance is deployed in Active Directory mode, the operation is handled by an Appliance Administrator in Active Directory and cannot be the built-in administrator.
3. Once the audit log is successfully uploaded from the appliance, it is deleted from the appliance. This action is important because when the appliance is deployed in DocuSign TSCP CA, this is the only mechanism for deleting audit logs from the server.
   If you do run this tool, the Appliance audit log grows and once it gets to its maximal size, the appliance will not provide service until this tool is executed.

The following table describes the available parameters for `AuditLogDownloadUtility`. If no parameter is provided, the user is guided through the process:

Parameter	Description
`/?`	Lists all input parameters and their descriptions.
`-o <Sign/Verify>`	Whether to download and sign the audit log or verify an existing signed audit log file. Default: Sign
`-del <0-no, 1-yes>`	Whether to delete the downloaded audit logs from the appliance as part of the download and sign operation. Audit logs will be deleted only after a successful sign operation. Default: 0 – No deletion of audit logs Note: It is highly recommended to delete information from the DocuSign SA audit log, otherwise the audit log can grow to the point that the Appliance stops providing services due to audit log flooding.
`-dir <output directory>`	Where to place the output, which is the signed audit logs. Defualt: the local directory

Parameter	Description
`-log <debug log file>`	Whether to output debug information to a debug log file. This information can be sent to DocuSign customer support if necessary. This parameter is optional.
`-IP <IP address>`	The IP address or DNS name of the DocuSign Signature Appliance. This parameter is optional.
`-A <Authentication kind>`	The type of authentication to use when accessing the appliance: 1 – SSPI 2 - Server side authentication 3 - SSPI User Password client side 4 - Push authentication
`-PN <Principal name>`	The DocuSign SA principal name for SSPI authentication. This parameter is optional. In the case of SSPI, this information is neglected.
`-adm <User name>`	The administrator name for authentication based on user name and password. This parameter is optional.
`-pwd <Password>`	The password for authentication based on user name and password. This parameter is optional and may be redundant when the user logs on in an Active Directory environment.
`-dom <Domain name>`	The domain name for authentication based on user name and password. This parameter is optional.
`-file <signed audit log file>`	The audit log file to be verified.

Note: If the utility does not receive the administrator login information, it will prompt you for the administrator user name and password.

Alerts regarding Audit Log size

If the DocuSign SA audit logs starts filling up, the following alerts appear in the Web Console:

- **The log is almost full (85%-90%)**

In this case, the following event is written to the event log: `Event log is 85% full.`
It is recommended to run the *AuditLogDownloadUtility.exe* utility which downloads the audit log, signs it, and deletes it.

- **The log is full (90%-99.5%)**

  In this case, the following event is written to the event log: `Event log is 90% full.`
  At this point the appliance will shutdown and the Appliance administrator will need to start it. All appliance services will still be available, but it is highly recommended to promptly run the *AuditLogDownloadUtility.exe* utility which downloads the audit log, signs it, and deletes it.

- **The log is full (99.5%)**

  In this case, the following event is written to the event log: `Event log is 100% full.`
  At this point the appliance will shutdown and the Appliance administrator will need to start it.
  The only enabled functionality of DocuSign SA will be to download the audit log, sign it and have it deleted. To do so, run the *AuditLogDownloadUtility.exe* utility.

Chapter 6: Using the DocuSign SA Console

This chapter describes how to connect to and use the DocuSign SA web-based console to manage DocuSign SA. The console enables operations that cannot be performed using the DocuSign SA Administration MMC. The console includes also a built-in touch screen for display purposes only.

Accessing the DocuSign SA Console

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.

Using the DocuSign SA 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.

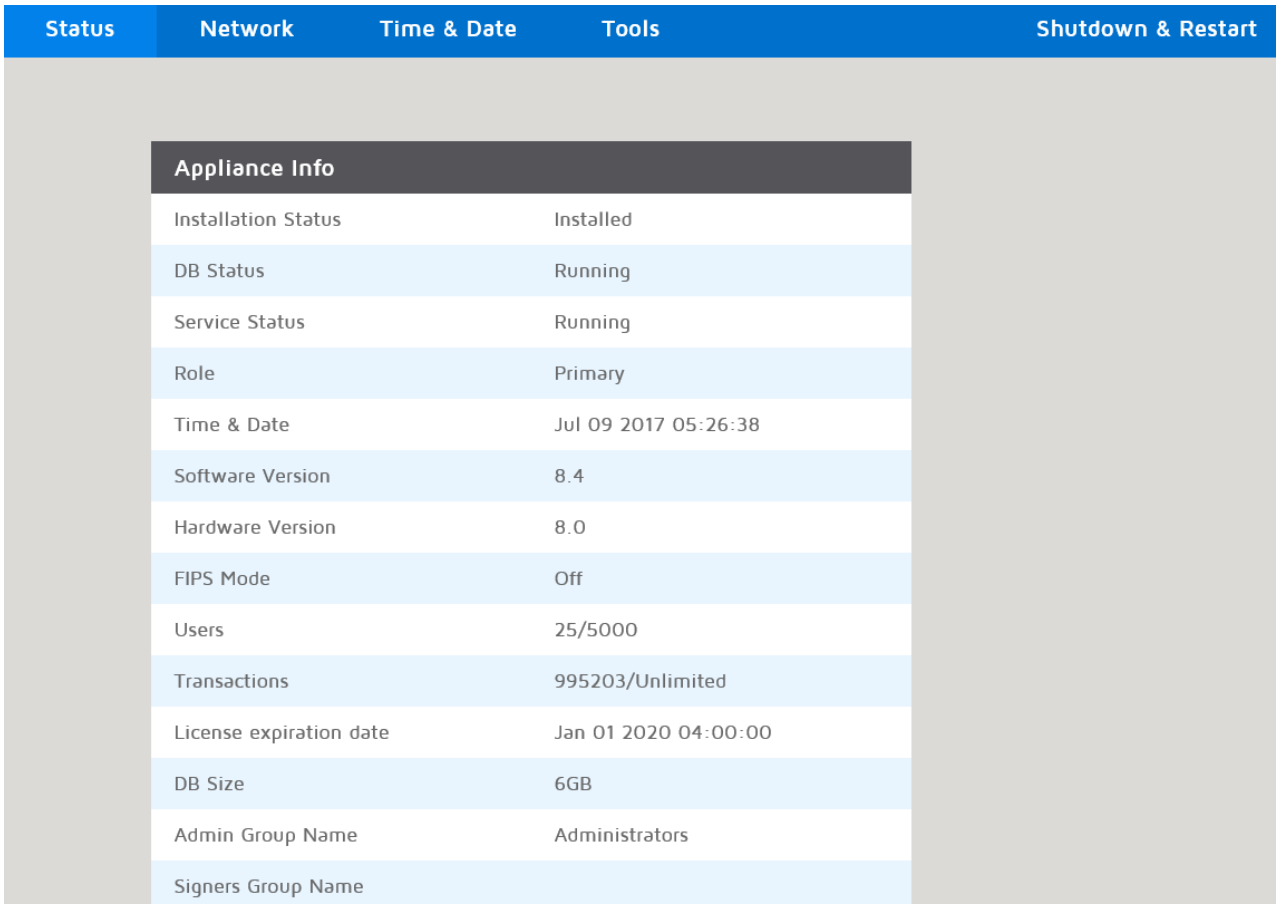


Figure 79 Web-based Console – Main Window

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:

1. Confirm the action. This results in appliance shutdown.

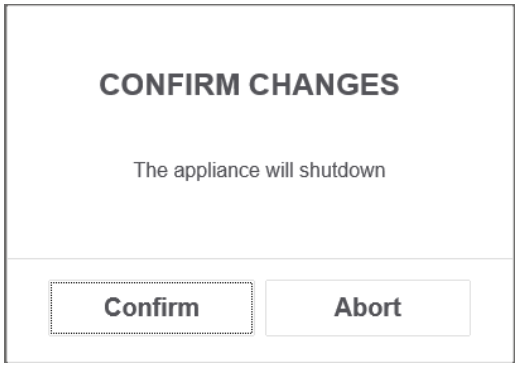


Figure 80 Web-based Console – Confirm Changes

2. Commit the changes by removing and re-inserting the license token in order to prove physical access to the appliance.

Note: The Microsoft Edge web browser does not work well with the DocuSign SA Web-based Console. It is therefore recommended to use the DocuSign SA Web-based Console in a Chrome browser.

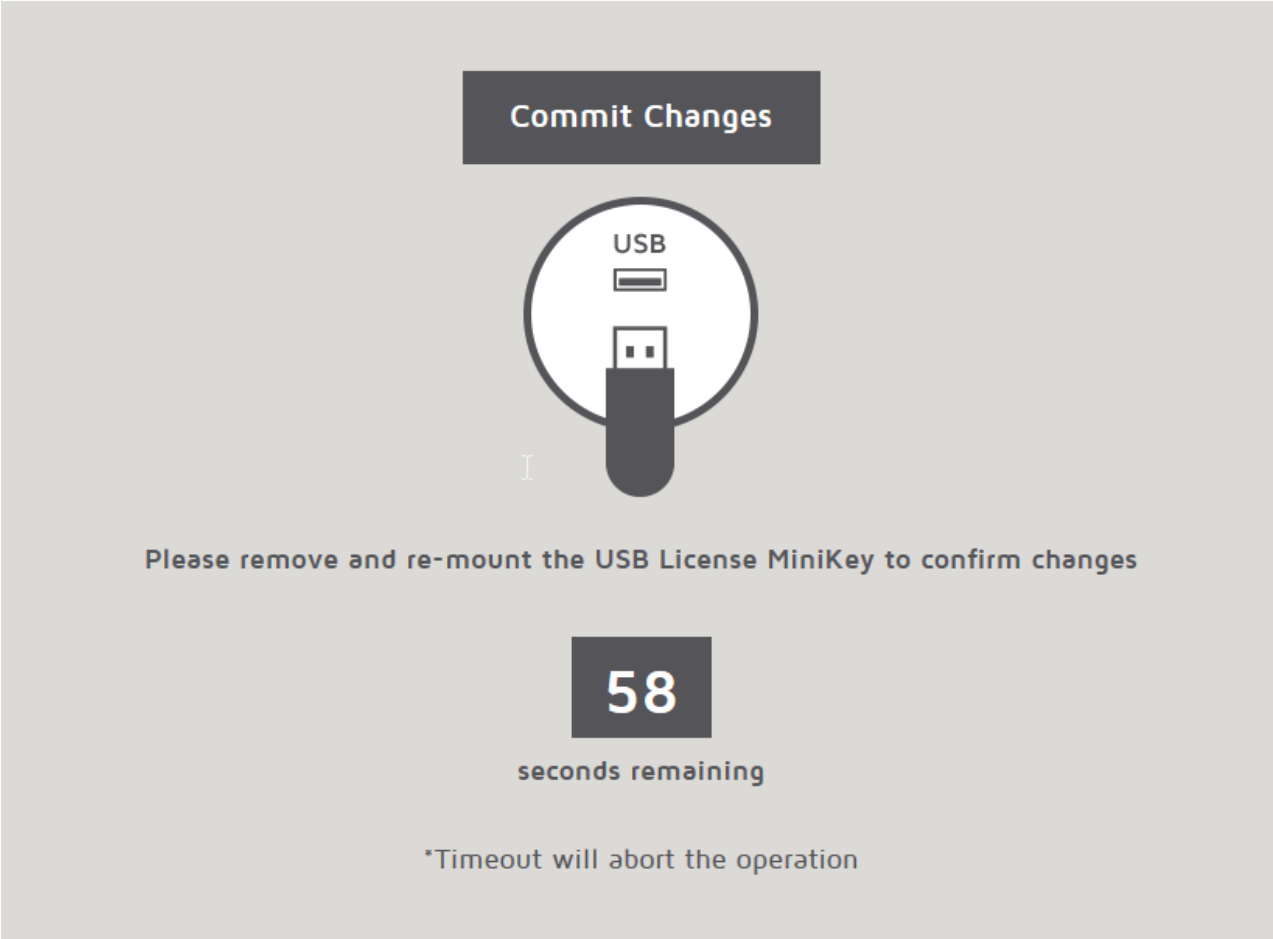


Figure 81 Web-based Console – Commit Changes

Setting the Appliance IP Address

To set the DocuSign SA IP address:

1. In the main window, select the **Network** tab.

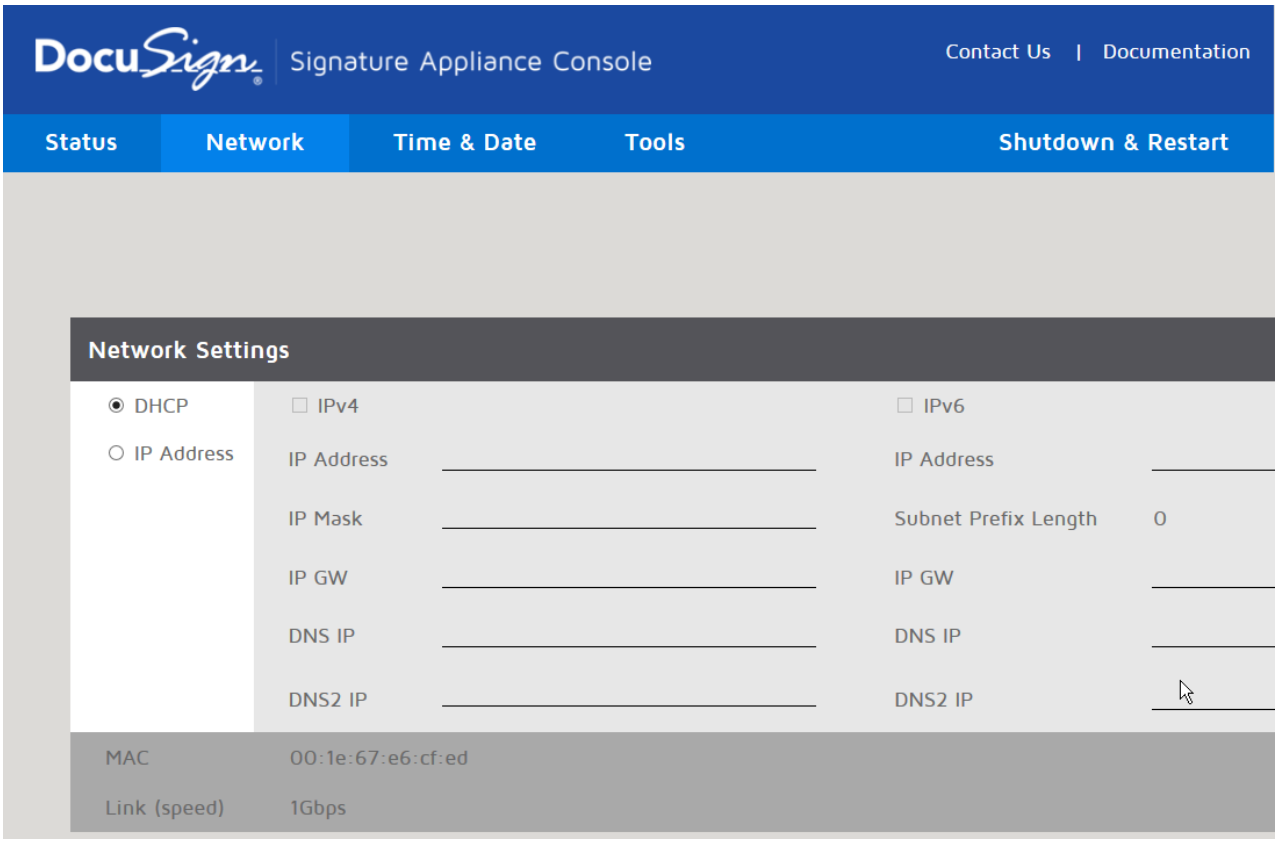


Figure 82 Web-based Console – Network tab

2. Specify whether the address will be supplied in **IPv4** or **IPv6** format.
3. 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 SA clock. This parameter is very important since it affects the effective start date of a user certificate generated by DocuSign SA, as well as affecting Active Directory user authentication.

You can modify the DocuSign SA time by either modifying the contents of DocuSign SA's date and time fields, or by specifying that DocuSign SA time will be constantly updated by the time of an NTP server.

To set the DocuSign SA time:

1. In the main window, select the **Time & Date** tab.

   The current time is displayed.

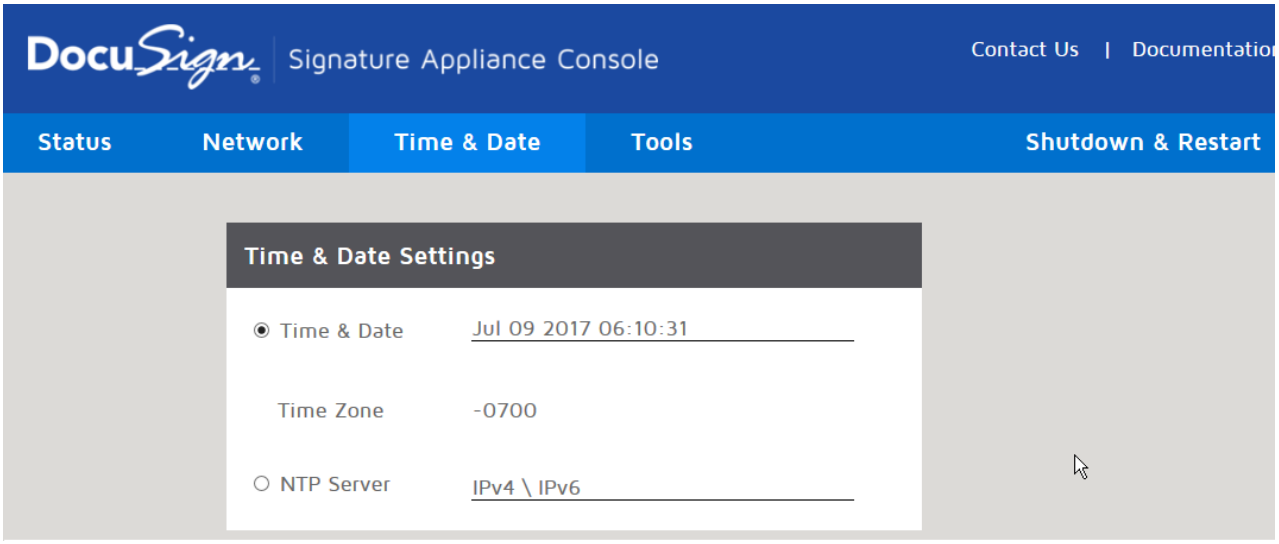


Figure 83 Web-based Console – Time & Date tab

2. 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.

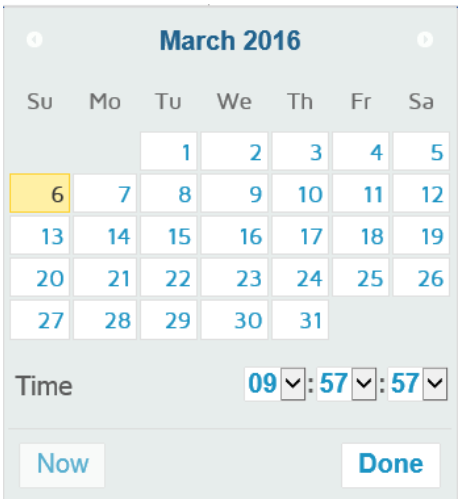


Figure 84 Setting DocuSign SA Time

Alternatively, you can specify an **NTP server** IP address. This option constantly updates the DocuSign SA 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 SA:

1. In the main window, select the **Shutdown & Restart** tab.

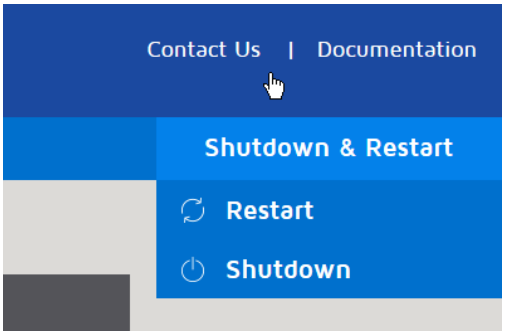


Figure 85 Web-based Console – Shutdown & Restart tab

2. In the Shutdown & Reset menu, select **Shutdown**.
3. Confirm the operation.

Restarting the Appliance

To restart the appliance:

1. In the main window, select the **Shutdown & Restart** tab (Figure 79).
2. In the **Shutdown & Reset** menu, select **Restart** (Figure 85).
3. Confirm the operation.

Resetting the Tamper Mechanism

To reset the tamper mechanism:

1. In the main window, select the **Tools** tab (Figure 79).
2. In the **Tools** menu, select **Reset tamper** (Figure 86).

Note: The **Reset Tamper** option appears only in a Tamper situation.

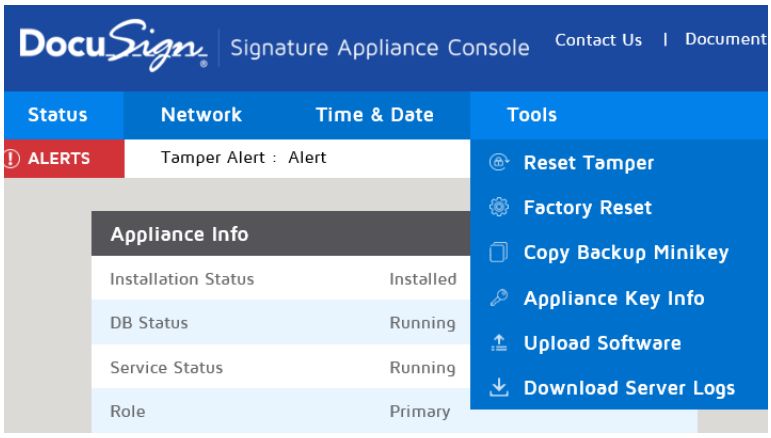


Figure 86 Web-based Console – Tools Menu – Reset Tamper

3. At the prompt, insert one of the backup MiniKey tokens. The following message appears:

   `Please insert a backup Minikey that was created during installation`

4. After the backup MiniKey is inserted, the following message appears:

   `Resetting tamper, please wait` …
   `Done.`

5. 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 SA with the Directory Service*.

Restoring Factory Settings

The console enables you to restore DocuSign SA to its factory settings. You may want to do this in any of the following circumstances:

- DocuSign SA was installed for demo, pilot, or development purposes, and you now want to reinstall the DocuSign SA software for production purposes.
- You want to reinstall the DocuSign SA software with different parameters.
- Installation failed or was stopped, and the DocuSign SA 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 SA.
- Unregisters DocuSign SA from the domain.
- Resets all DocuSign SA 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 DocuSign SA computer from the Active Directory. To fully unregister the DocuSign Signature Appliance, manually remove the DocuSign SA computer from the Active Directory.

To restore factory settings:

1. In the main window, select the **Tools** tab (Figure 79).
2. In the **Tools** menu, select **Factory Reset** (Figure 87).
3. Confirm the operation.

Copying the Backup Minikey

This option enables you to create another copy of the backup Minikey token.
This option is not available when the DocuSign SA is deployed in Common Criteria EAL4+ mode.

To create a new copy of the backup Minikey token:

1. In the main window, select the **Tools** tab (Figure 79).
2. In the **Tools** menu, select **Copy Backup Minikey**.

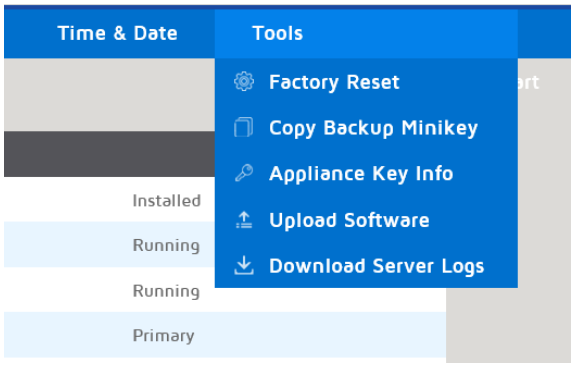


Figure 87 Web-based Console – Tools Menu

3. In the notification window that appears, click **Continue**.

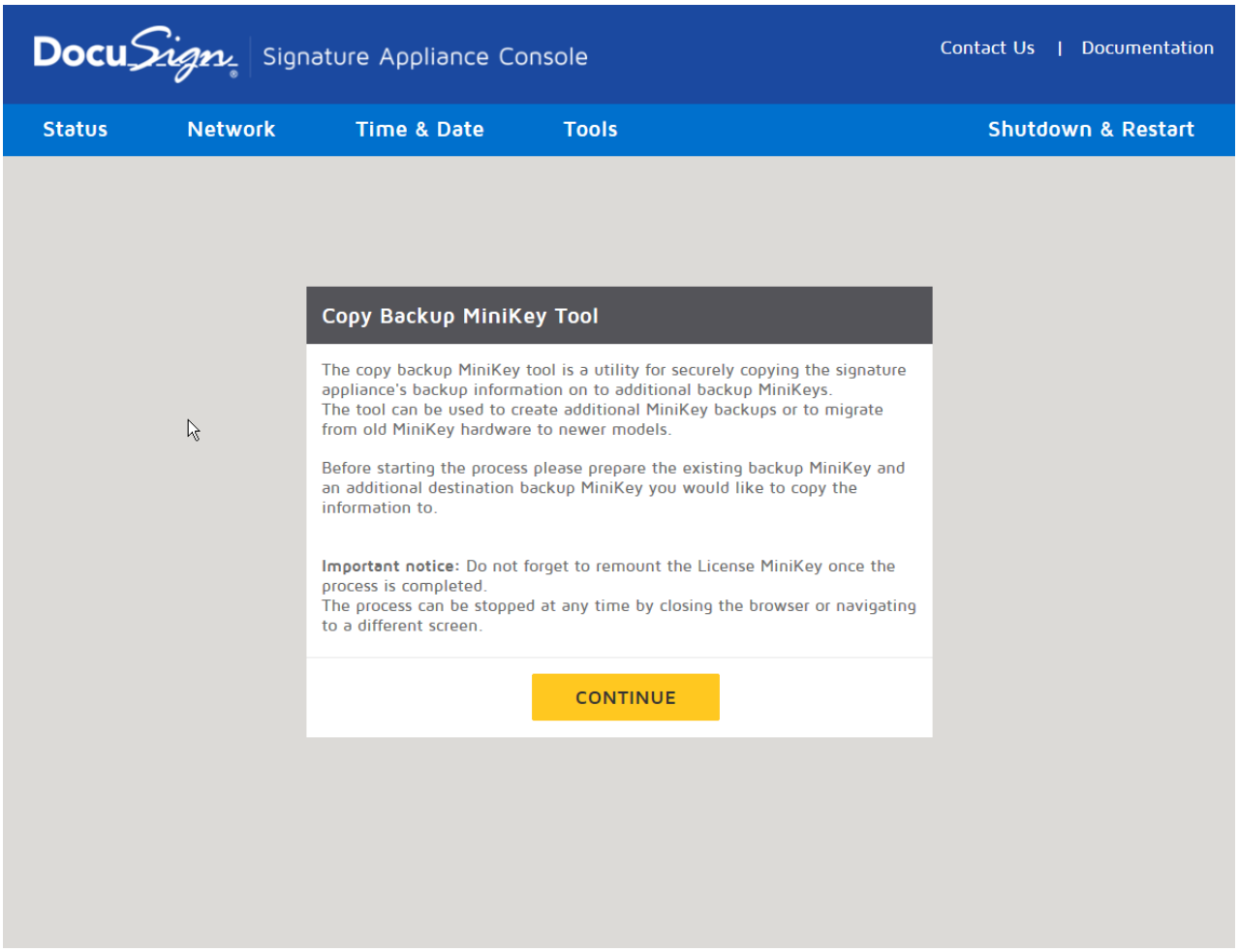


Figure 88 Web-based Console – Copy Backup MiniKey Tool

A window appears, requesting you to insert one of the original backup tokens.

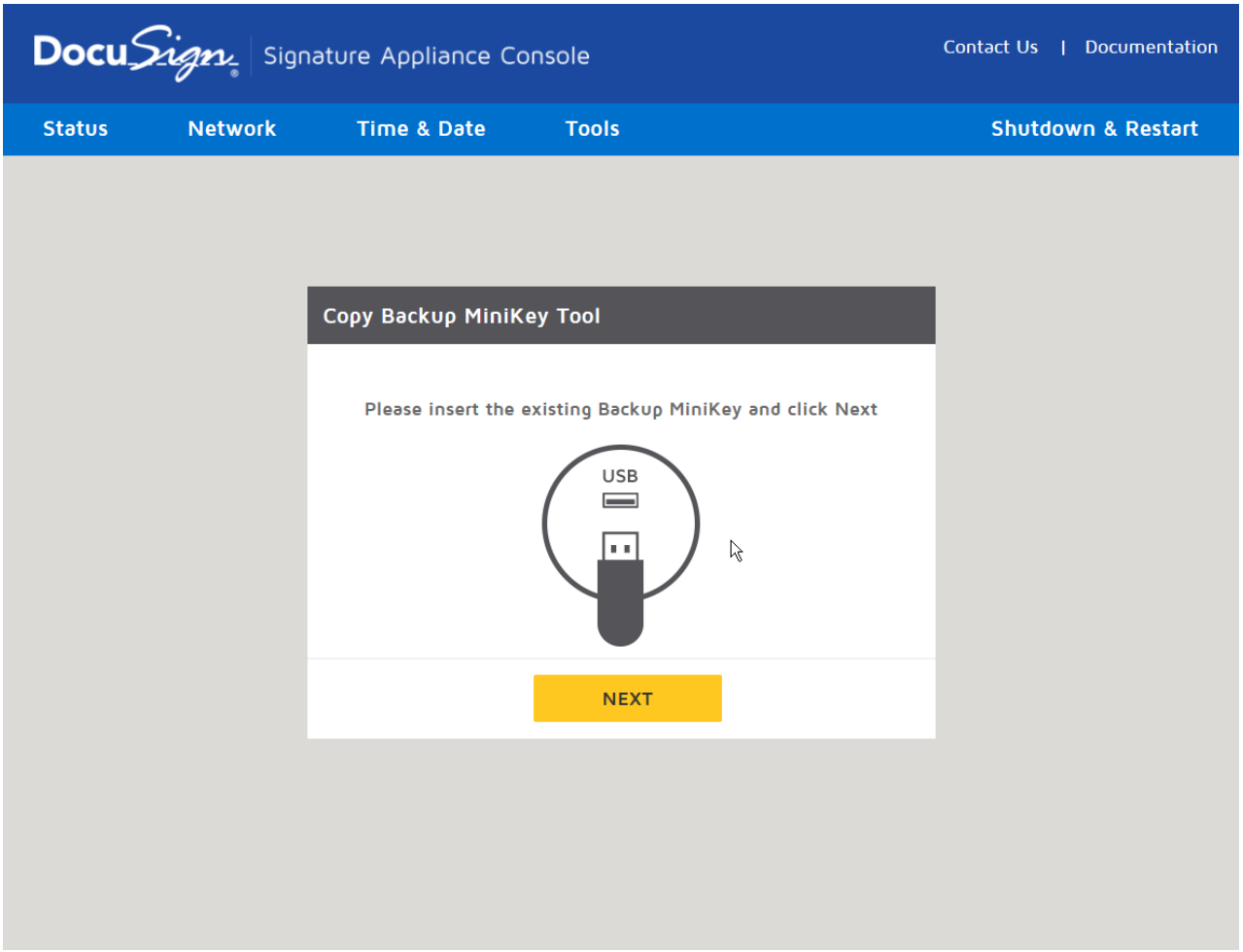


Figure 89 Web-based Console –Insert Backup MiniKey

4. Insert one of the original backup tokens and click **Next**.

   A window appears, acknowledging the inserted Backup Minikey and requesting you to insert a blank backup Minikey.

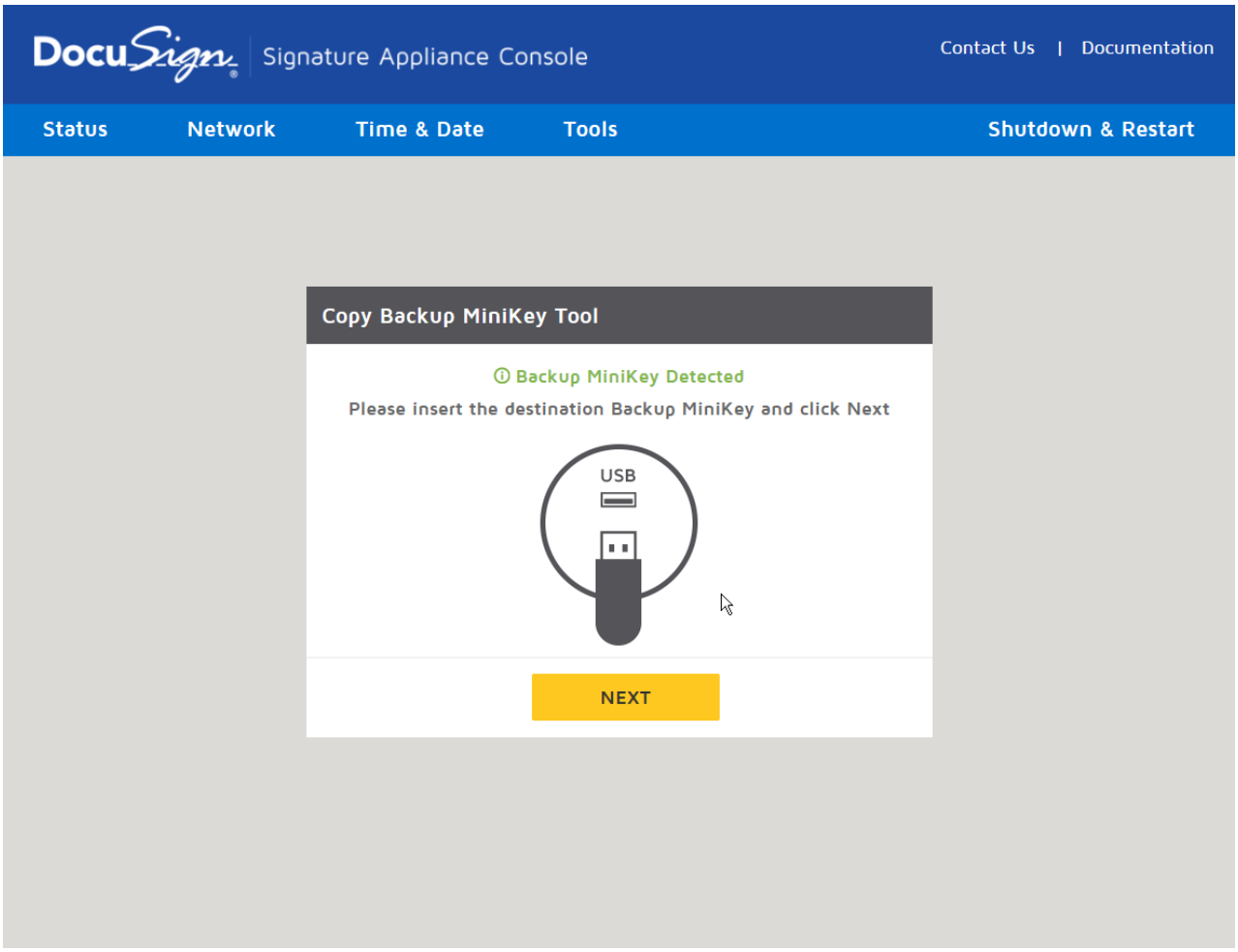


Figure 90 Web-based Console – Insert a Blank Destination Backup Minikey

5. Insert a blank backup Minikey and click **Next** to perform the copy operation.

A success notification appears.

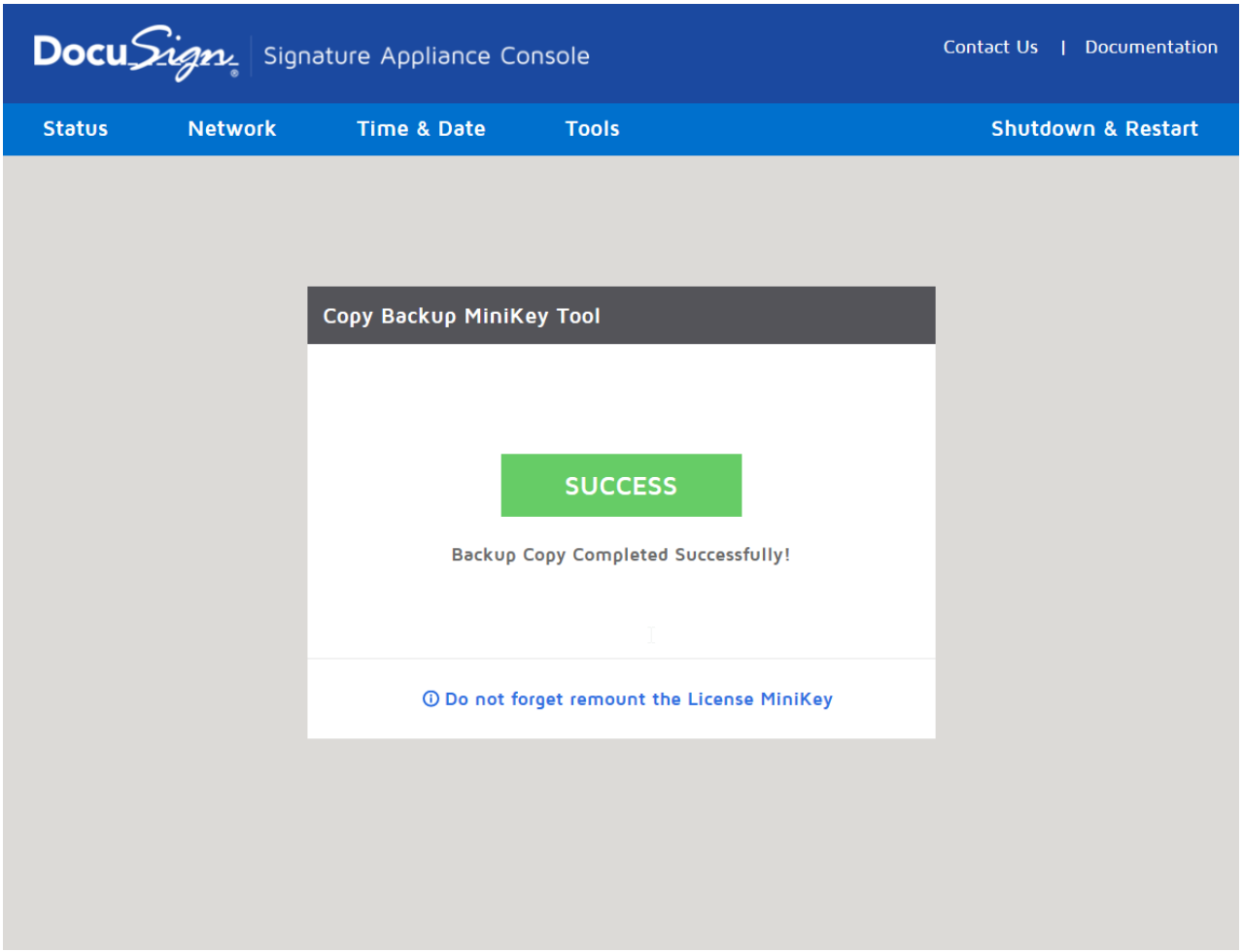


Figure 91 Web-based Console – Backup Copy Completed Successfully

Checking whether Security Information in the Appliance Matches Security Information in the Minikey Token

This option enables you to check whether the Appliance secret information matches the information inside the backup Minikey.

To check for a security information match:

1. Insert the backup Minikey token.
2. In the main window, select the **Tools** tab (Figure 79).
3. In the **Tools** menu, select **Appliance Key Info** (Figure 87).

   The Appliance Key Info window appears:

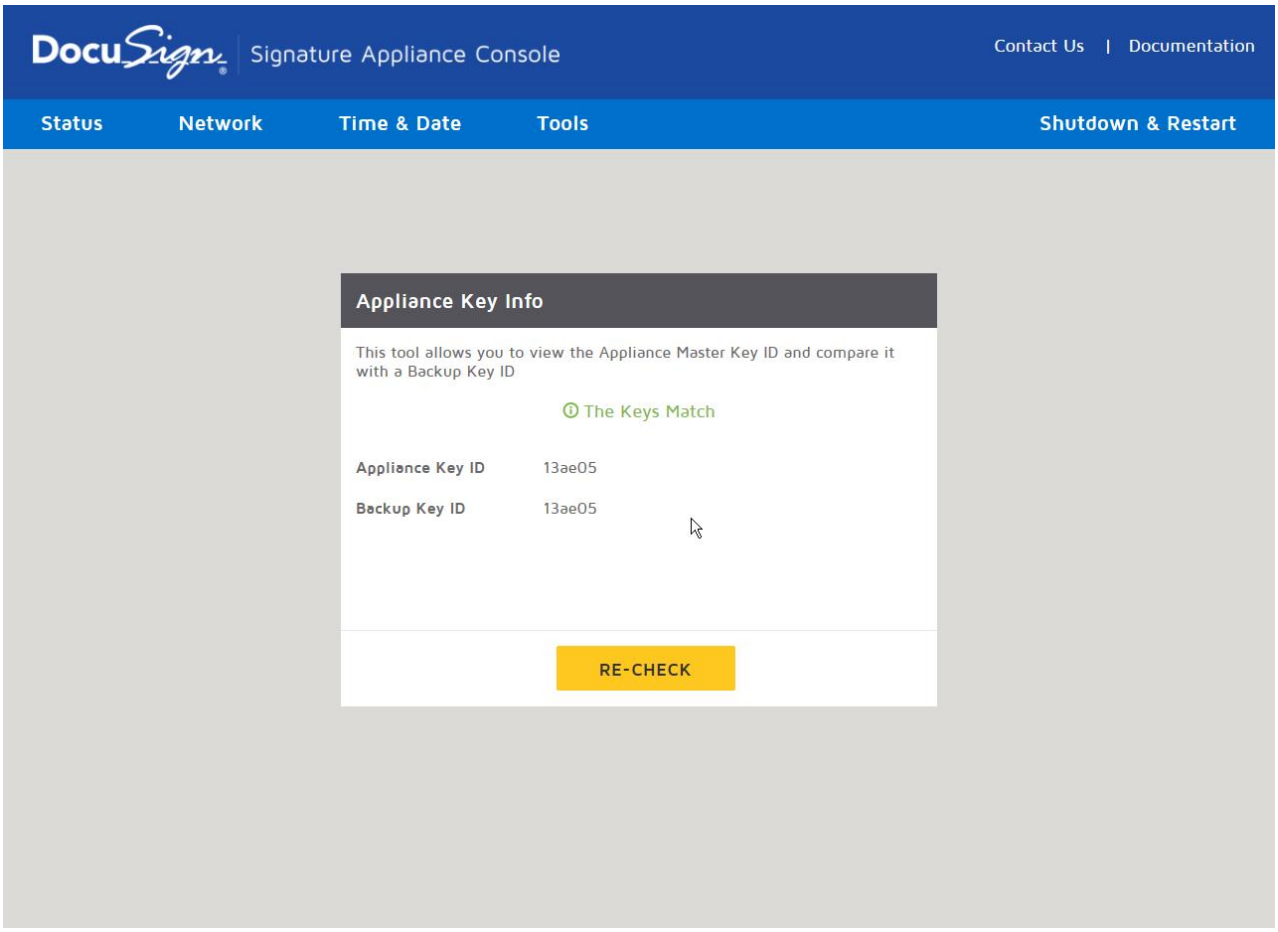


Figure 92 Web-based Console – Appliance Key Info

4. If the 6 characters of the **Appliance Key ID** and the 6 digits of the **Backup Key ID** are identical, this means that the security information inside the Appliance and inside the backup Minikey is identical.

Upload Software

Use this option only if instructed to do so specifically by DocuSign Support.

This option is equivalent to uploading software fixes through the DocuSign Signature Appliance Management. This option will be used only if there are technical issues that prevent loading fixes in the customary fashion (as described in *Upgrading*).

To upload software:

1. In the main window, select the **Tools** tab (Figure 79).
2. In the **Tools** menu, select **Upload Software** (Figure 87).
3. Remove and insert the License Token to prove physical access to the Appliance.
4. In the screen that appears, browse to the software package (.dlm file).

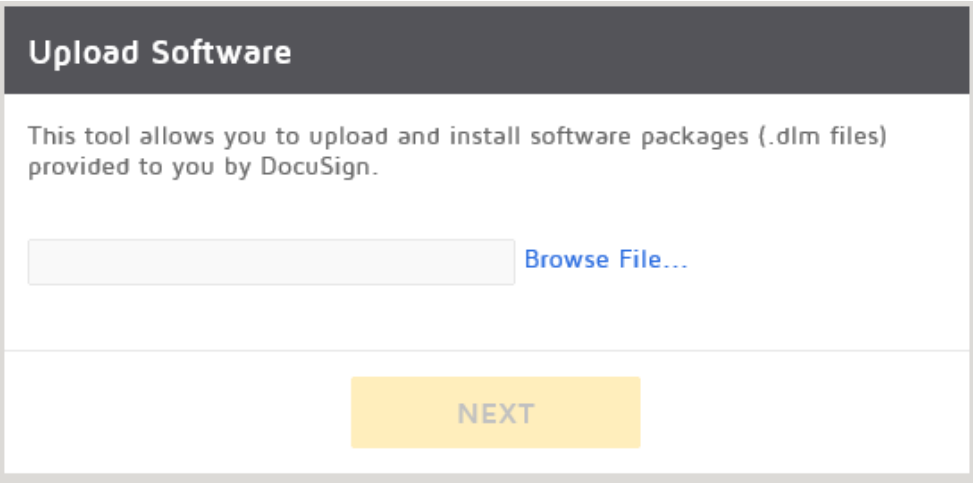


Figure 93 Web-based Console – Appliance Key Info

5. Click **Next**.

   The .dlm file is loaded and installed. Upon Success, a Success message is displayed.

Download Server Logs

Use this option only if instructed to do so specifically by DocuSign Support.

This option downloads Appliance technical log files through the DocuSign Signature Appliance Management. It provides detailed technical information that is required by DocuSign support for analysis of technical issues.

To download server log files:

1. In the main window, select the **Tools** tab (Figure 79).
2. In the **Tools** menu, select **Download Server Logs** (Figure 87).
3. Remove and insert the License Token to prove physical access to the Appliance.

   The log files will be downloaded to the Administrator's desktop.

Displaying DocuSign Signature Appliance Status

To display DocuSign Signature Appliance status:

1. In the main window, select the **Status** tab (Figure 79).

   The Status tab appears, displaying Appliance Info and Networking information.

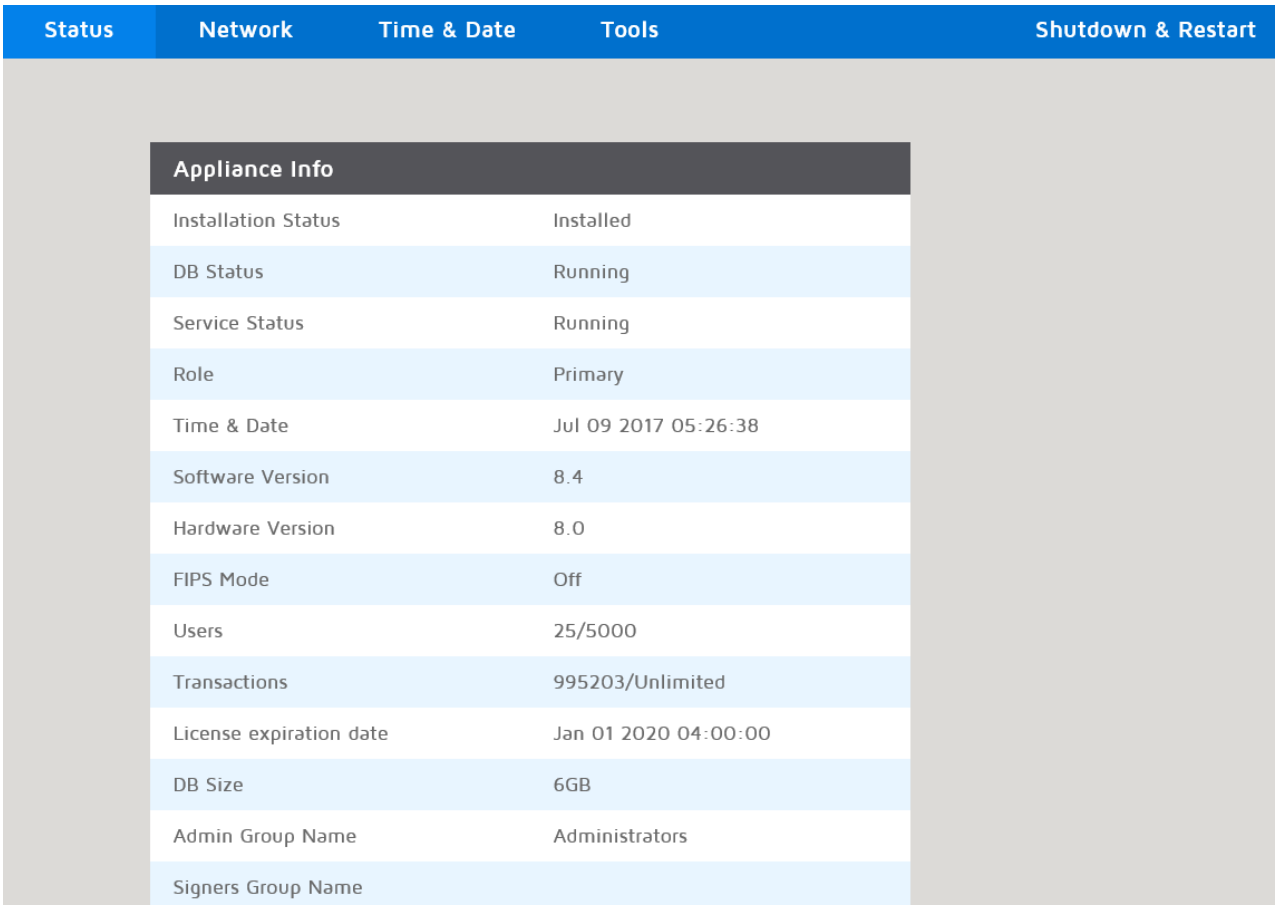


Figure 94 Web-based Console – Status tab – Appliance Info

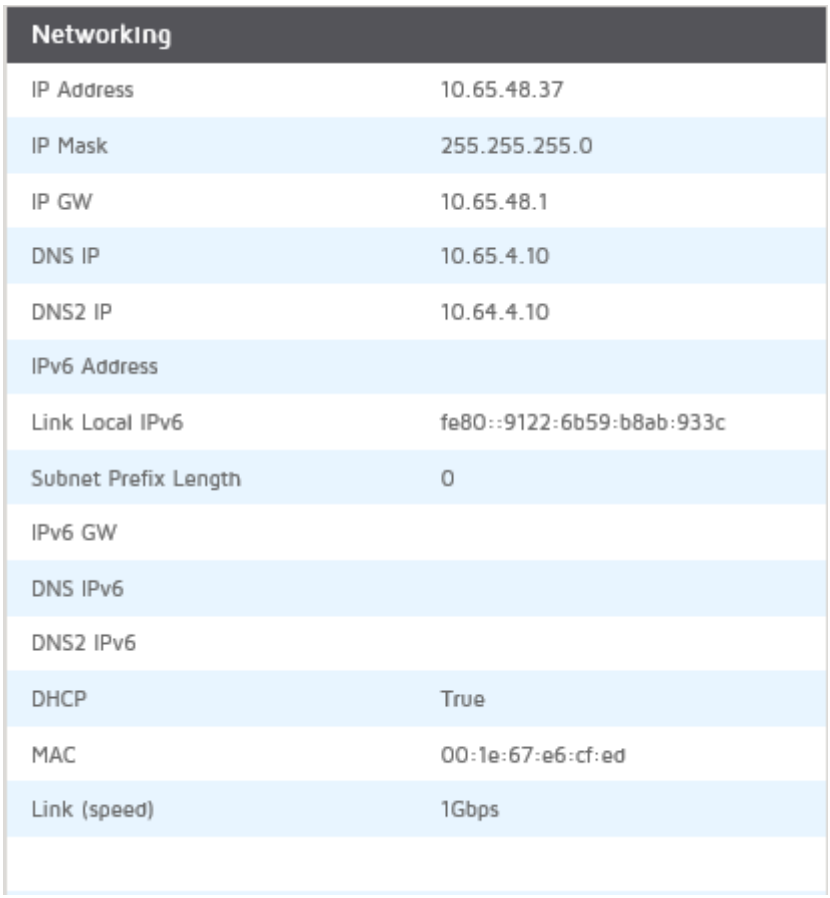


Figure 95 Web-based Console – Status tab – Networking

The following table describes the DocuSign Signature Appliance status information parameters:

Parameter	Description
Installation Status	The installation status of the DocuSign Signature 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 DocuSign SA database. Possible values: Running, Starting, Stopped, Stopping.
Service Status	The status of the DocuSign SA 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).

Parameter	Description
Software Version	The DocuSign Signature Appliance software version. This parameter also includes the Master Disk version, which indicates the underlying inner operating system version.
Hardware Version	The DocuSign SA 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 SA 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. ♦ *RESTful Web Services Support* is set to False ♦ **Replication communication mode** is set to **IPSec**. Refer to *Setting the Communication Protocol between the Primary Appliances and Alternate Appliances* ♦ *Disable 3DES in TLS* 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 *Infinite* is displayed. Otherwise, the expiration date is displayed.
DB size	The size of the DocuSign SA database files.
Admin group Name	The name of the directory users group whose members are allowed to manage DocuSign SA via the DocuSign SA Administration MMC.
Signers group Name	The name of the directory users group whose members are users of DocuSign SA when DocuSign SA is installed in AD mode.
WWV Certs Status	Indicates the status of the CA certificate authority, whether it is DocuSign CA, DocuSign TSCP CA or Symantec CA. The status is either *Service Down* or *Service Up*. If the status is *Service Down* please contact DocuSign Support. In addition, the expiration date of the RA key is indicated as follows *Exp: <date>*. If the RA key is close to its expiry date , please contact DocuSign for renewing the RA key.
Signers WWV Cert Pend	The number of pending certificate requests when DocuSign SA interfaces with an External CA in Automated mode. This parameter is relevant only when Comodo is deployed.

Parameter	Description
Serial Number	The serial number of the DocuSign Signature Appliance.
IP Address	IP address of the DocuSign Signature Appliance, in IPv4 format.
IP Mask	Subnet mask of the DocuSign Signature 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.
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 DocuSign Signature Appliance.
Link (speed)	The network connectivity state. Possible values: 10Mb, 100Mb, 1Gb.

Using the Touch Screen of a DocuSign SA 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.

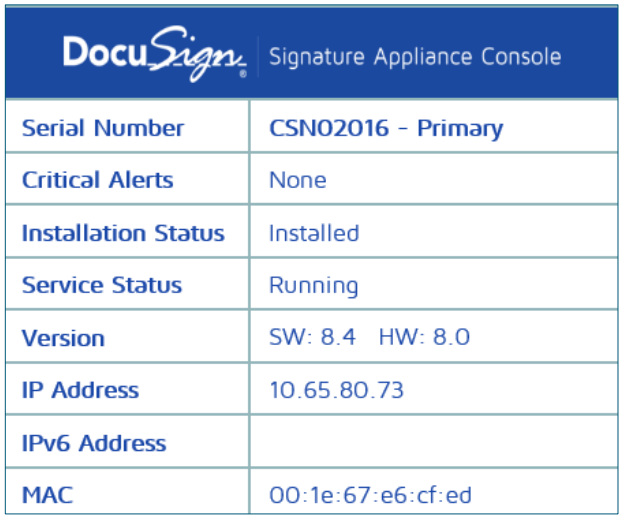


Figure 96 Appliance Touch Screen

Errors such as tamper or license problems are displayed in the **Critical Alerts** line.

Restoring the DocuSign Signature Appliance after an Internal Hard Disk Failure

In Appliance Hardware v8.1 Enterprise model

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 DocuSign SA software from booting and running normally.

This option should be used only if the DocuSign SA console does not reach the regular operating Menu and instead displays *DocuSign SA 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 DocuSign technical support before performing a comprehensive factory restore.

To perform a comprehensive factory restore:

1. Restart the appliance.
2. When the appliance starts, the following message appears for two seconds: *Press the service key to enter the service console*.
3. Press button 1.

   The Service menu is activated.

4. A *please select* message appears, prompting you to select between **Quit** and **Restore**.
5. Select **Restore**.

   Note: If you select ***Quit***, the DocuSign Signature Appliance continues to boot in the normal fashion.

   A final caution message appears: **Restoring will erase all existing data. Are you sure?**
6. Select **Yes**.

   Note: If you select ***No***, the DocuSign Signature Appliance continues to boot in the normal fashion.

   The Comprehensive Restore operation begins. The entire content of the DocuSign SA firmware, including the data, is restored using a disk image that was created by DocuSign during DocuSign SA manufacturing.

   You can now perform a restore operation using an existing backup file, or perform a new installation.

In DocuSign SA Hardware V8.0 – Appliance FIPS model

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 DocuSign SA software from booting and running normally.

This option should be used only if the DocuSign SA console does not reach the regular operating Menu and instead displays *DocuSign SA 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 DocuSign technical support before performing a comprehensive factory restore.

To perform a comprehensive factory restore:

1. Restart the appliance and connect a keyboard to the USB port.
   In the case of a DocuSign SA Enterprise appliance, connect a monitor as well.
2. When the appliance starts, the following message appears for two seconds:
   *Press **S** to start the service console*.
3. Press the **S** keyboard key.

   The Service menu is activated.
4. A *please select* message appears, prompting you to select between **quit(Q)** and **restore(R)**.
5. Select **Restore**.

   Note: If you select ***quit(Q)***, the DocuSign Signature Appliance continues to boot in the normal fashion.

A final caution message appears: **Restoring will erase all existing data. Are you sure Y/N?**

6. Select **Yes(Y)**.

> ***Note:*** If you select ***No(N)***, the DocuSign Signature Appliance continues to boot in the normal fashion.

The Comprehensive Restore operation begins. The entire content of the DocuSign SA firmware, including the data, is restored using a disk image that was created by DocuSign during DocuSign SA 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 DocuSign Signature Appliances to provide the following:

- *Redundancy* – If a DocuSign Signature Appliance is not available, the other DocuSign Signature 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 DocuSign Signature Appliances can be used in parallel to improve performance.

This chapter provides an overview of the DocuSign SA high availability configuration, followed by a detailed description of how to set up the DocuSign SA system for high availability functionality.

Overview of High Availability

To enable a DocuSign SA 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 DocuSign Signature Appliance*, and the other DocuSign Signature Appliances in the site are defined as *alternate DocuSign Signature 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 DocuSign SA 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 CA, the primary DocuSign Signature Appliance communicates with the External CA to obtain end user certificates.

The administrative operations can only be performed in the primary DocuSign Signature Appliance, therefore if the primary DocuSign Signature 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 DocuSign SA 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 DocuSign SA 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.
You can define a different IPSEC protocol that can be used when the Appliance works in FIPS mode. This configuration is not relevant when the DocuSign Signature Appliance is deployed in CC EAL4+ mode.

Client behavior in a high availability configuration:

In a high availability configuration, the DocuSign SA 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 SA Information through the SCP*.

For information about configuring the appliance in the client settings, refer to the Client – Appliances section in the *DocuSign SA Configuration Utility* chapter of the *DocuSign SA 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.

Deployment in Common Criteria mode:

When DocuSign SA is deployed in Common Criteria mode (either as a Signature Creation Device or as a Seal Creation Device), only the Primary Appliance can be accessed by clients. The Alternate Appliance(s) are deployed for the purpose of replication.

In the case of a temporary fatal error at the Primary Appliance (perhaps as the result of an electrical problem, or a local networking problem), it is possible to define, in advanced, a specific alternate appliance that will provide the digital signature service to users until the Primary DocuSign Signature Appliance is analyzed and is back in service.

Special networking infrastructure such as special routers can be deployed for the purpose of monitoring the Primary Appliance and determining when it is in a temporary fatal error.
In such case, the networking based requests will be forwarded to the selected alternate appliance.

Installing DocuSign Signature Appliances in a High Availability Configuration

In a high availability configuration, the order of installation is as follows:

1. Install the primary DocuSign Signature Appliance.
2. Install the alternate DocuSign Signature Appliances.

The following sections describe the installation process.

> ***Note:*** Both the Primary Appliance and the Alternate Appliances in a cluster must have the same hardware version and software version.
>
> Please make sure that all hardware versions and software versions of DocuSign Signature Appliances you receive from DocuSign and are intended to be deployed in the same cluster are the same.
>
> Whenever it is required to upgrade the software version of the Primary Appliance, please make sure that you upgrade the software versions of all Alternate Appliances as well.

Installing the Primary DocuSign Signature Appliance

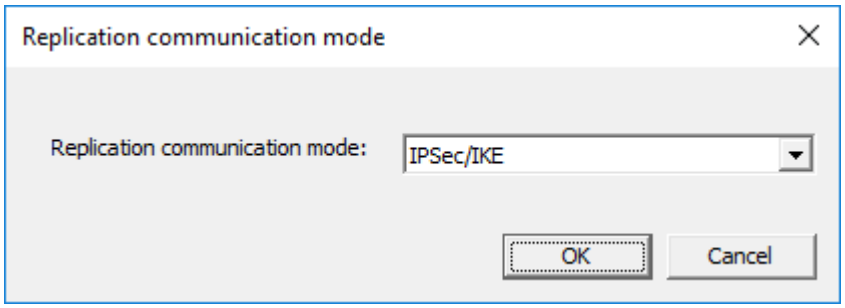
Installing a primary appliance is identical to installing a stand-alone DocuSign Signature Appliance (refer to *Installing the DocuSign Signature Appliance Hardware version 8.0* and *Installing the DocuSign Signature Appliance Software*). During software installation, the administrator specifies the user management environment (i.e., Active Directory or Directory Independent).

Setting the Communication Protocol between the Primary Appliances and Alternate Appliances

The communication protocol can be configured to enable the DocuSign Signature Appliance to be set in FIPS mode. This is done by setting the replication communication mode. You need to perform the following operations for every appliance in the cluster (the primary appliance and all alternate appliances).

To set the replication communication mode for working in FIPS mode:

1. In the *DocuSign Signature Appliance Management* window (*Figure 100*), right-click the relevant DocuSign Signature Appliance whose replication communication mode you wish to change.
2. From the popup menu, select **All Tasks → High Availability → Set replication communication mode**. The *Replication Communication Mode* window appears.



3. In the *Replication communication mode* window, change the value of **Replication communication mode** to **IPSec** if you would like the appliance to work in FIPS mode.

   When the DocuSign Signature Appliance is deployed in Common Criteria EAL4+ mode, it is mandatory to set this parameter to IPSEC/IKE.

   The default mode is IPSec/IKE.

Installing an Alternate DocuSign Signature Appliance

The following sections describe the hardware and software installation of an alternate DocuSign Signature Appliance.

Installing the Alternate DocuSign Signature Appliance Hardware

Prepare the alternate DocuSign Signature Appliance for installation, and perform the hardware installation of the appliance, as described in *Installing the DocuSign Signature Appliance Hardware version 8.0*.

Installing the Alternate DocuSign Signature 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 SA. Refer to *Installing DocuSign SA in a Microsoft Active Directory Environment*.

To install the alternate DocuSign Signature Appliance software:

1. In the system tray, right-click the icon and select **Administrative Tools → Appliances Management**. The *DocuSign Signature Appliance Management* window appears.
2. Login to the DocuSign Signature Appliance using either the built-in administrator or another admin account.
3. Right-click the primary DocuSign Signature Appliance, select **All Tasks**, and then select **High Availability → Install Alternate**.
4. The *Network setup* dialog box appears.

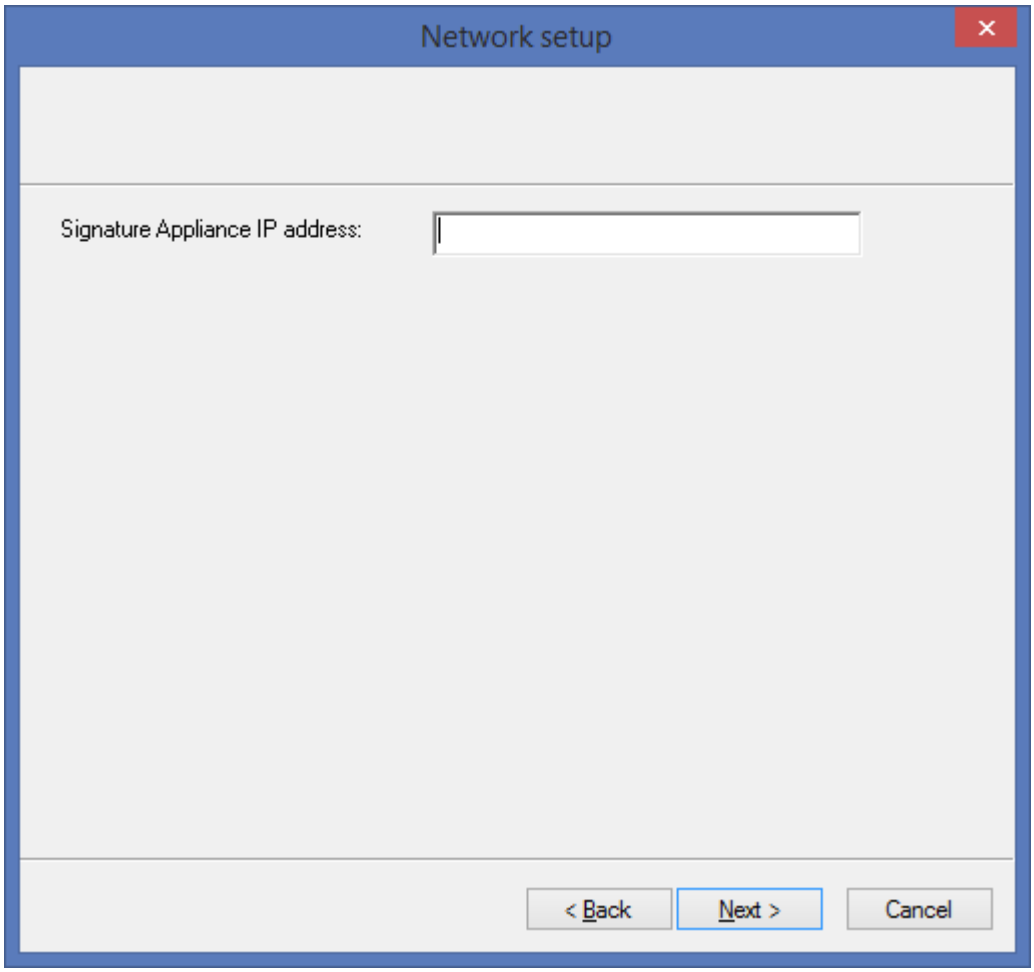


Figure 97 Network Setup Dialog Box

Enter the IP address of the alternate DocuSign Signature Appliance. This parameter is necessary for enabling basic communication to and from the DocuSign Signature Appliance.

Note: For information on setting up the IP address of the DocuSign Signature Appliance, refer to *Setting the Appliance IP Address*.

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.

5. In the case of an Active Directory installation, enter the user name and password of an administrative account with permission to join the alternate DocuSign Signature Appliance to the domain.

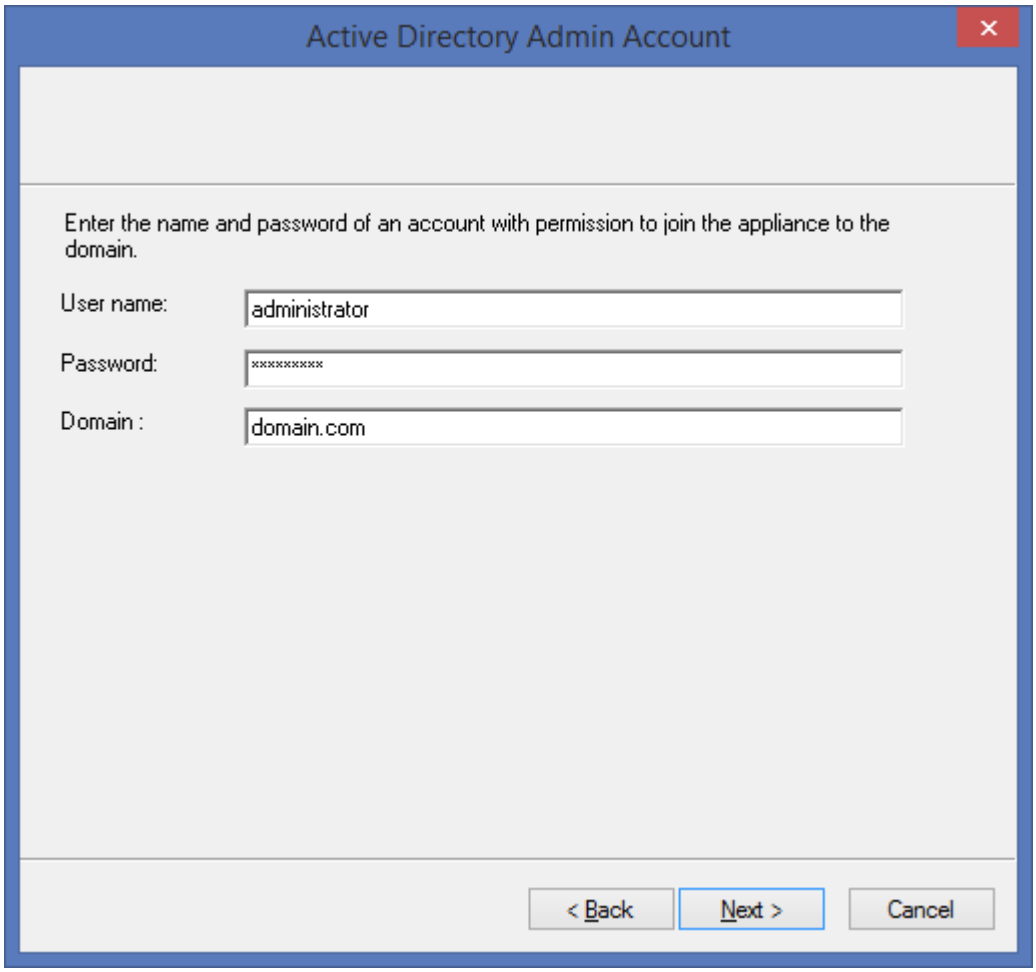


Figure 98 Active Directory Admin Account Dialog Box

6. Click **Next**. DocuSign SA 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 DocuSign SA 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 DocuSign Signature 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 DocuSign Signature Appliance and the alternate DocuSign Signature Appliance, which will cause the replication to fail.

7. 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 DocuSign Signature Appliance. For example, if four DocuSign Signature Appliances are installed in the same site, each of the DocuSign Signature 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 DocuSign Signature Appliance database is copied over the network to the alternate DocuSign Signature Appliance.

   Note: Please do not press **Cancel** at this stage since this will cause the Alternate Appliance not to be installed correctly, and you will need to re-install it.

8. At the end of the installation, the following message appears:

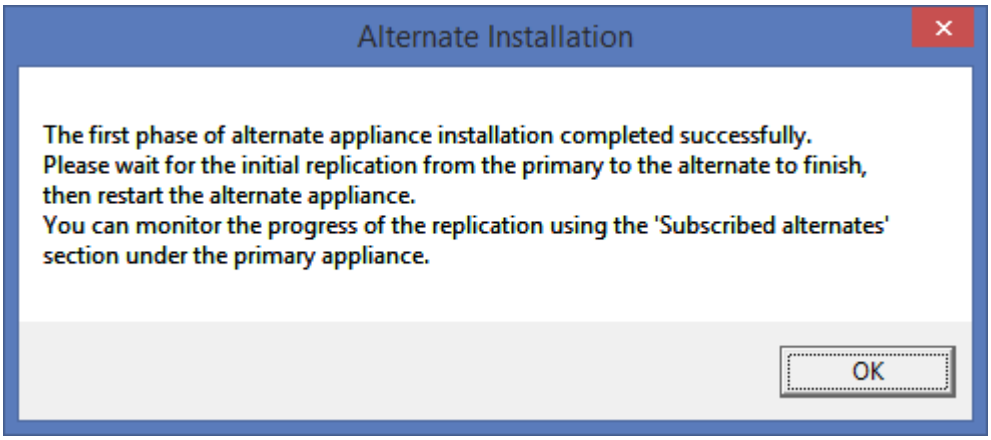


Figure 99 Initial Replication Message

   Data replication between the primary DocuSign Signature Appliance and the alternate DocuSign Signature Appliance continues after DocuSign SA alternate installation ends.

9. Click **OK**.

   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 SA to factory settings and then try again. For more information about restoring factory settings, refer to *Restoring Factory Settings*.

10. In the *DocuSign Signature Appliance Management* window, right-click **DocuSign Signature Appliances** and select **Refresh** from the popup menu. The window refreshes and displays the newly installed alternate appliance.

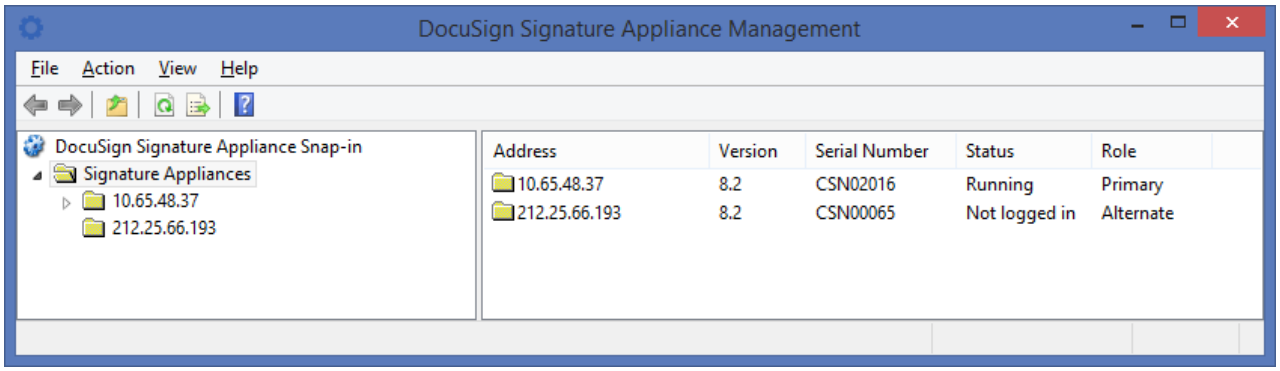


Figure 100 DocuSign Signature Appliance Management Window – Displaying Primary and Alternate Appliances

11. Verify that all data was indeed replicated to the alternate DocuSign Signature Appliance (refer to *Managing Data Replication in the Alternate DocuSign Signature Appliance*). The replication state should be OK (refer to *Viewing Replication Status of an Alternate DocuSign Signature Appliance*).
12. Perform a hard restart of the alternate DocuSign Signature Appliance. The restart ensures that the alternate DocuSign Signature Appliance starts using replicated data, such as system parameters; otherwise, unexpected results may occur.

The alternate DocuSign Signature Appliance is ready for use.

Managing the Alternate DocuSign Signature Appliance

Some management operations are disabled for an alternate DocuSign Signature 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 DocuSign SA service or the DocuSign Signature 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 *DocuSign Signature Appliance Management* window of the DocuSign SA 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 DocuSign Signature Appliance fails and is later re-installed from backup, all alternate appliances must be re-installed as well.

Managing Data Replication in the Alternate DocuSign Signature Appliance

You can view and manage data replication using the DocuSign SA 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 DocuSign Signature Appliance installation, since the replication procedure continues after installation is complete.

To view and manage data replication, select **Subscribed Alternates** under the primary DocuSign Signature Appliance.
The *Subscribed Alternates* window that appears lists the alternate DocuSign Signature Appliances.

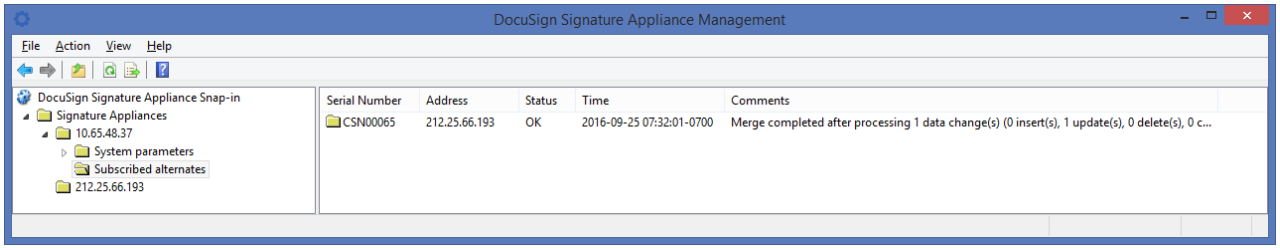


Figure 101 Subscribed Alternates Window

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 DocuSign Signature Appliance

The Subscribed Alternates window (Figure 101) in the DocuSign SA Administration MMC displays the time of the last replication activity accompanied by descriptive text. It also displays the following information about each alternate DocuSign Signature Appliance: the DocuSign SA Serial Number, the IP Address and the Status.
The possible statuses include:

- **OK** – No data needs updating in the alternate DocuSign Signature Appliance.
- **Running** – The alternate DocuSign Signature Appliance is currently synchronizing with the database of the primary DocuSign Signature Appliance.

- **Retrying** – The primary DocuSign Signature Appliance is trying to communicate with the alternate DocuSign Signature Appliance, but cannot reach it due to network problems or because the alternate DocuSign Signature Appliance is not installed.
- **Failed** – Replication has failed. This occurs after several failed retry attempts.

Re-initializing an Alternate DocuSign Signature Appliance

The Subscribed Alternates window in the DocuSign SA Administration MMC enables re-initializing an alternate DocuSign Signature Appliance. This forces a replication operation in which all the relevant data of the primary DocuSign Signature Appliance is copied to the alternate DocuSign Signature Appliance.

Re-initialization can be used in cases where replication failed due to transient network problems.

To re-initialize an alternate DocuSign Signature Appliance:

1. In the **Subscribed Alternates** window (Figure 101), right-click the DocuSign Signature Appliance you wish to re-initialize.
2. From the popup menu, select **All Tasks** → **Re-initialize**.

Unsubscribing an Alternate DocuSign Signature Appliance

The Subscribed Alternates window in the DocuSign SA Administration MMC enables unsubscribing an alternate DocuSign Signature Appliance. This removes the **alternate** DocuSign Signature Appliance from the list of Subscribed Alternates. Use this option when an alternate appliance is no longer relevant in the site of the primary DocuSign Signature Appliance, or before re-installing the alternate appliance.

To unsubscribe an alternate DocuSign Signature Appliance:

1. In the **Subscribed Alternates** window (Figure 101), right-click the DocuSign Signature Appliance you wish to unsubscribe.
2. From the popup menu, select **All Tasks** → **Unsubscribe**.
3. 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.

4. In the *DocuSign Signature Appliance Management* window (*Figure 100*), right-click the alternate DocuSign Signature Appliance you wish to set as primary.
5. 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.

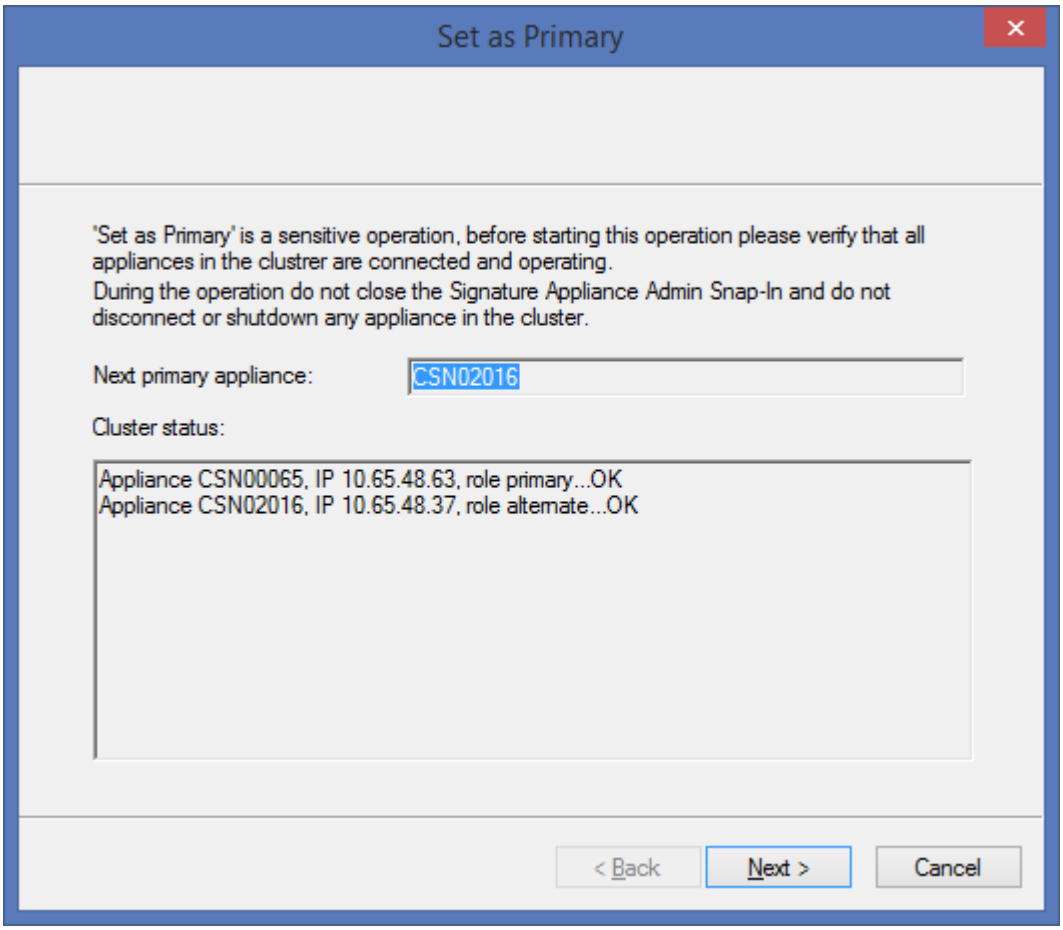


Figure 102 Set as Primary – Cluster Status

6. Click **Next** and confirm the operation.

   A progress window appears, and the operation of switching the role of primary to the alternate appliance begins.

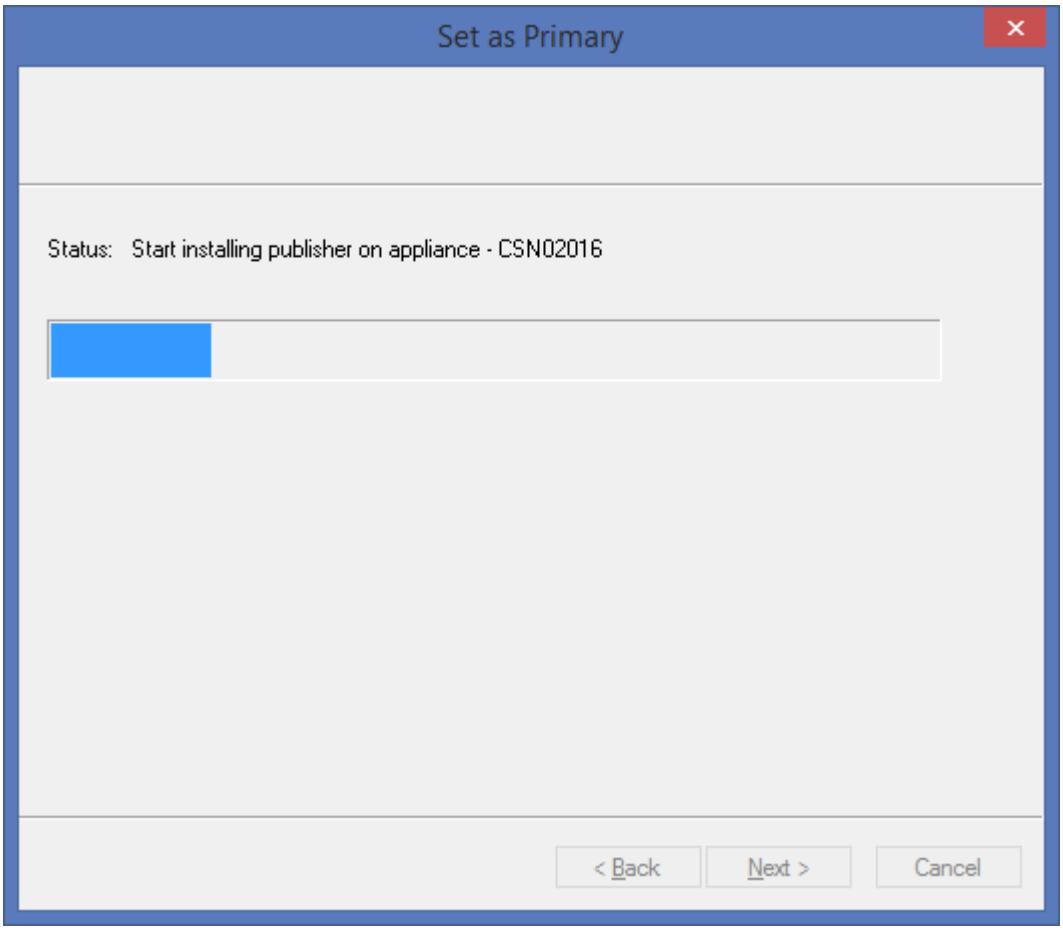


Figure 103 Set as Primary – Start installing the alternate as a primary

At the end of the operation a report is displayed, describing the performed actions. If you suspect any failure in the operation, contact DocuSign support.

7. 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:

1. In the *DocuSign Signature Appliance Management* window (*Figure 100*), right-click the previous primary DocuSign Signature Appliance that you wish to designate as an alternate.
2. 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.

Re-subscribing an Alternate Appliance with a Primary Appliance

There are cases where an alternate appliance is unsubscribed from a primary appliance, and you wish to re-subscribe 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:

1. In the *DocuSign Signature Appliance Management* window (*Figure 100*), right-click the primary DocuSign Signature Appliance to which you wish to subscribe an alternate appliance.
2. 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.
3. Enter the IP address of the alternate appliance.
4. 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 SA.

To upgrade appliances in a high availability cluster:

1. Unsubscribe all alternate appliances from the primary appliance (refer to *Unsubscribing an Alternate*).
2. In the Subscribed Alternates window (*Figure 101*), make sure that no alternate appliances are listed for the primary appliance.
3. Upgrade the primary appliance (refer to *Upgrading*). Wait until the upgrade is complete.
4. 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 DocuSign SA console shows the updated version number.

5. Subscribe each alternate appliance to the primary appliance (refer to *Re-subscribing an Alternate Appliance with a Primary Appliance*).

The high availability cluster is now upgraded and ready for operation.

Chapter 8: DocuSign SA Configuration Utility

The DocuSign SA client behavior in general and each DocuSign SA 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 DocuSign SA Configuration Utility enables both the user and the administrator to set the configuration of any parameter in any of the DocuSign SA client components both for a single machine and for a group of machines.

User related functionality is described in the *DocuSign SA User Guide*.

Overview

The DocuSign SA Configuration Utility is a GUI application that enables a user or administrator to set any of the DocuSign SA client components' configurable parameters easily and intuitively.

The DocuSign SA 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 DocuSign SA 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 DocuSign SA Configuration utility is not the only method for changing the DocuSign SA client's behavior. Some of the components have their own GUI for setting their own configuration (such as the DocuSign SA Legacy Word Add-in plug-in, Prepare & Sign, and others), but while the components' GUI changes the setting of the current user, the DocuSign SA Configuration utility changes the configuration of the local machine.

You can also use the DocuSign SA Configuration Utility to retrieve the DocuSign SA internal CA certificate and the DocuSign SA CA CRL (Certificate Revocation List).

Using the DocuSign SA Configuration Utility

The DocuSign SA Configuration Utility enables you to view and edit all the configurable parameters of the DocuSign SA 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 DocuSign SA client components. Refer to *Running the DocuSign SA Configuration Utility in Admin Mode* and *Running the DocuSign SA Configuration Utility in End User Mode* for more information about the two modes.

To run the DocuSign SA Configuration Utility:

- To run in **Admin** mode, in the tray right click the icon, and select **Administrative Tools** > **Client Configuration Management** (Figure 53). The DocuSign SA configuration utility main window appears.
- To run in **End User** mode, in the tray right click the icon, and select **Client Configuration** (Figure 53). The DocuSign SA configuration utility main window appears.

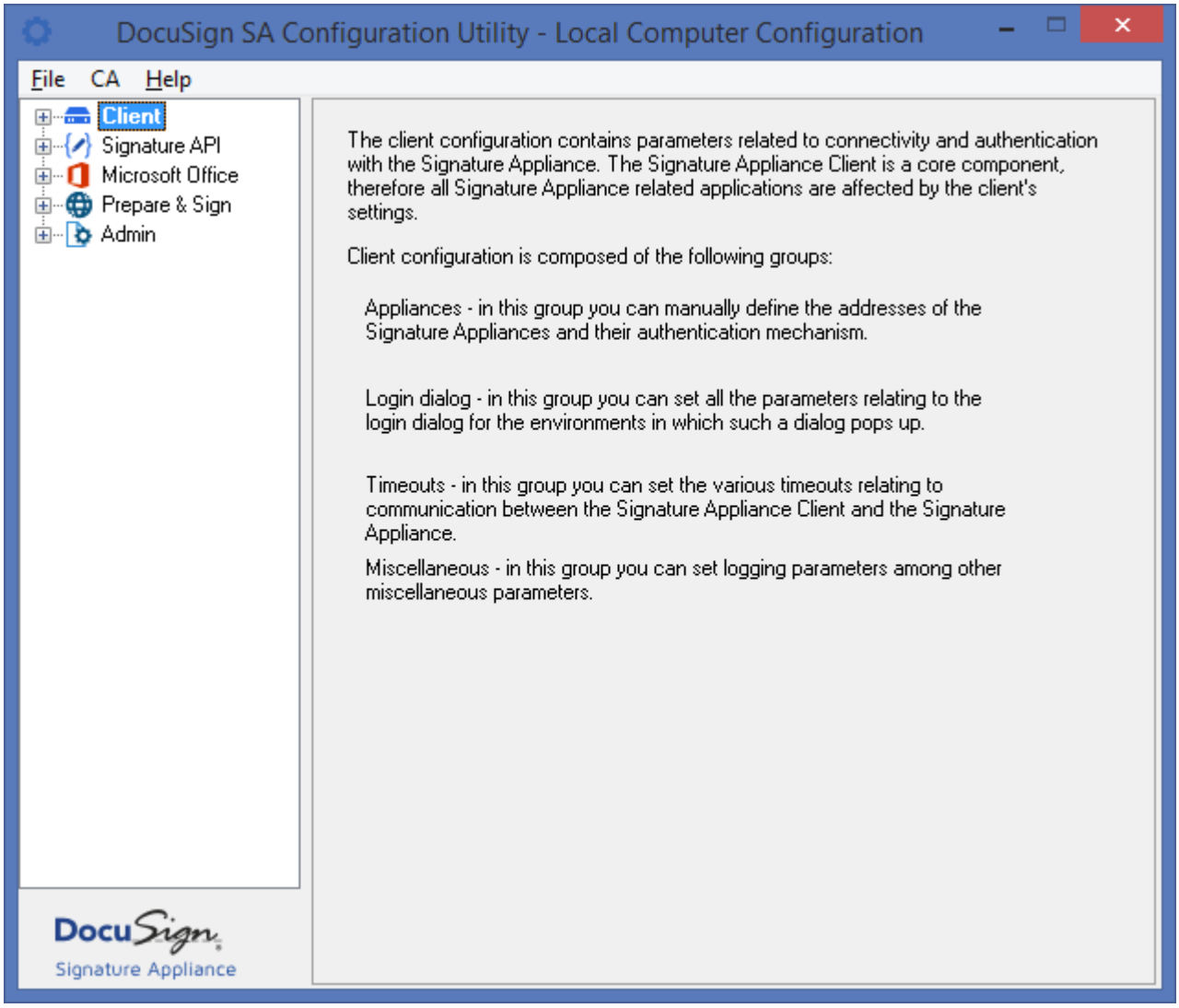


Figure 104 DocuSign SA Configuration Utility – Main Window

The left pane of the DocuSign SA 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:

1. Double-click the component to which this parameter belongs, or click ⊞ to the left of the component. The component's sub-nodes are displayed.
2. 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.
3. 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 DocuSign SA 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 DocuSign SA components:

     - *Client*. For explanations about the configurable parameters, refer to the DocuSign SA Configuration Utility chapter in the *DocuSign SA User Guide*.
     - *Signature API*. For explanations about the configurable parameters, refer to the DocuSign SA Configuration Utility chapter in the *DocuSign SA User Guide*.
     - *Microsoft Office*. For explanations about the configurable parameters, refer to the DocuSign SA Configuration Utility chapter in the *DocuSign SA User Guide*.
     - *DocuSign SA Prepare & Sign*. For explanations about the configurable parameters, refer to the DocuSign SA Configuration Utility chapter in the *DocuSign SA User Guide*.
     - *Admin*. For explanations about the configurable parameters, refer to *Setting Admin Configuration*.

DocuSign SA Configuration Utility Menus

The following sections describe the menu options available from the DocuSign SA 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.

> ***Note***: 32 bit Windows System are not supported.

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.

> ***Note***: 32 bit Windows System are not supported.

CA Menu

The following options are available from the **CA** drop-down menu:

Install DocuSign SA CA Certificate

Enables installing DocuSign SA's ROOT certificate into the current user's PC. Refer to *Chapter 4: Deploying the DocuSign SA Client* for information relating to DocuSign SA's ROOT certificate.

Download DocuSign SA CA Certificate

This option is very similar to the **Install DocuSign SA CA Certificate** option. The difference is that in this case the DocuSign SA 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 DocuSign SA CA CRL

Enables downloading the DocuSign SA 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 DocuSign SA configuration utility as well as a link to the DocuSign 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 DocuSign SA Client installation and the DocuSign Signature Appliance installation. Click **Save** to save the report to a file. The file can be sent to DocuSign support for problem analysis.

The report includes three parts:

- DocuSign SA Client installation files – Includes all the files of the DocuSign SA installation, their dates, sizes and version information.
- DocuSign SA Client and Server parameters – Includes DocuSign SA Client and Server parameters. The parameters also include information that is displayed in the DocuSign SA console.
- Environmental information – Displays information about the PC in which the DocuSign SA client is installed, the version of the installed MS Office application, and other parameters that can be valuable to DocuSign support for problem analysis.

Running the DocuSign SA Configuration Utility in Admin Mode

Note: To run the DocuSign SA Configuration Utility in Admin mode, you must first install the DocuSign SA admin client. Refer to *Installing DocuSign SA in a Directory Independent Environment*.

To run the DocuSign SA Configuration Utility in Admin mode:

1. In the system tray, right-click the  icon and select **Administrative Tools** > **Client Configuration Management** (Figure 53).

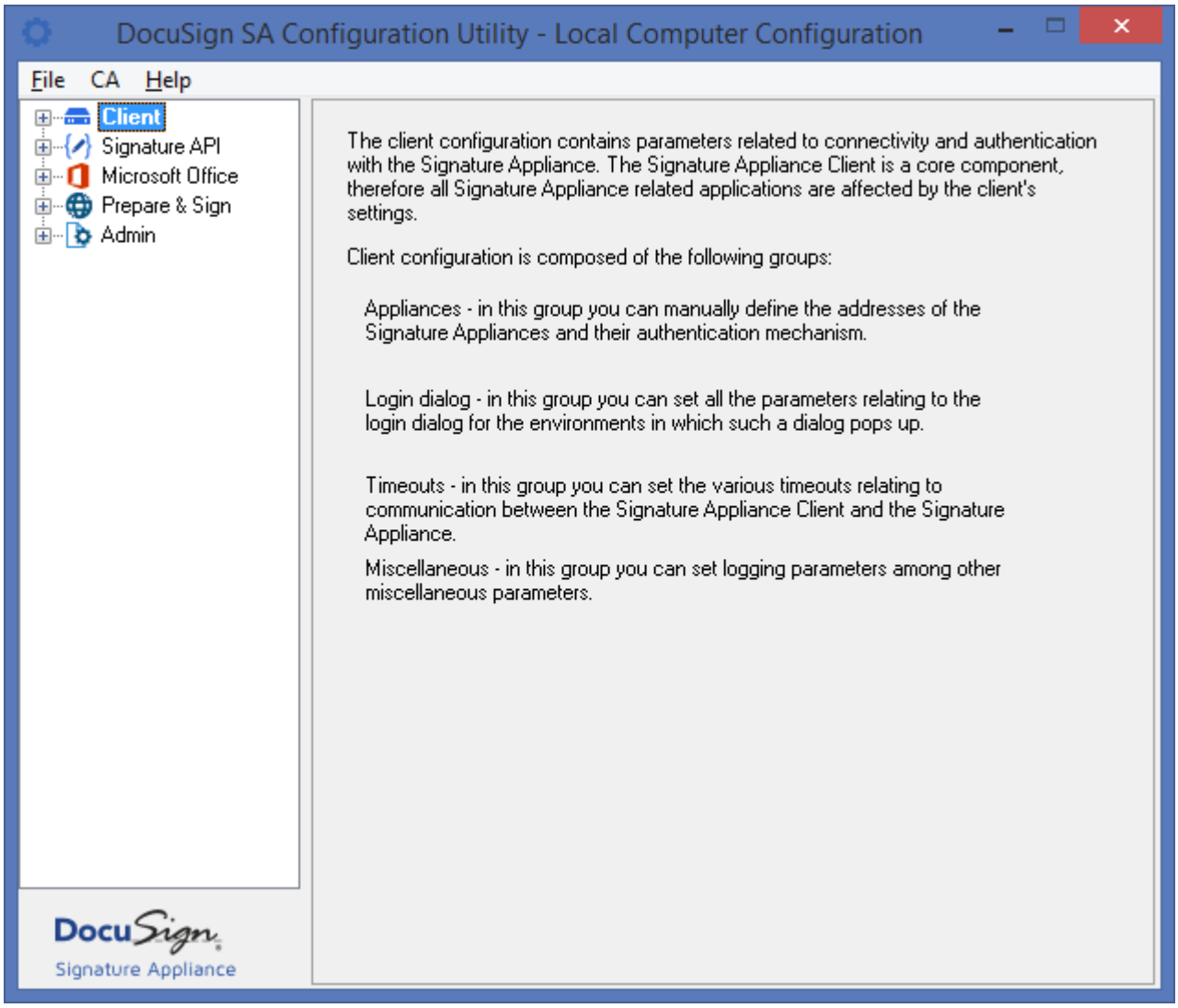


Figure 105 DocuSign SA Client Configuration Utility – Admin Mode

2. Edit the parameters as described in *Using the DocuSign SA Configuration Utility*.

   When running in *Admin* mode, all the DocuSign SA client configurable components are displayed in the left pane, regardless of the DocuSign SA 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 DocuSign SA Configuration Utility enables administrators to create and edit configuration files and to add and edit DocuSign SA 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 DocuSign SA Configuration Utility in *Admin* mode:

- Edit and save a configuration file.
- Edit/view a configuration file and export the DocuSign SA client settings to an existing Active Directory Group Policy.
- Edit/view the DocuSign SA settings of a Group Policy and save them in the same Group Policy or export them to another Group Policy.
- Edit/view the DocuSign SA settings of a Group Policy and export them to a configuration file.
- Install/Download the DocuSign SA CA certificate. Refer to *Install DocuSign SA CA Certificate* and *Download DocuSign SA CA Certificate*.
- Download the DocuSign SA CA CRL (Certificate Revocation List). Refer to *Download DocuSign SA 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 DocuSign SA Configuration Utility enables you to view and edit DocuSign SA related parameters in a Group Policy.

Opening a Group Policy

The DocuSign SA Configuration Utility can be used to open and edit the DocuSign SA setting in an existing Group Policy. Note that only the DocuSign SA 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 DocuSign SA 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 DocuSign SA Configuration Utility in End User Mode

The DocuSign SA 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 DocuSign SA 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 SA User Guide*.

Distributing the DocuSign SA Client Configuration

The DocuSign SA 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 DocuSign SA 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 DocuSign SA client configurations:

- Use DocuSign SA defaults – Do nothing except install the DocuSign SA client from the DocuSign SA CD. All users will have the same default behavior.
- Use the components' GUI – For each configured machine, use the DocuSign SA components' GUI to configure each component (Office Signature plug-in, DocuSign SA Prepare & Sign) 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 DocuSign SA Configuration Utility in *End User* mode – Run the DocuSign SA 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 DocuSign SA Configuration Utility. Refer to *Distributing the DocuSign SA 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 DocuSign SA Configuration Using Group Policy*.

Distributing the DocuSign SA Configuration Using Configuration Files

The configuration files created by the DocuSign SA 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:

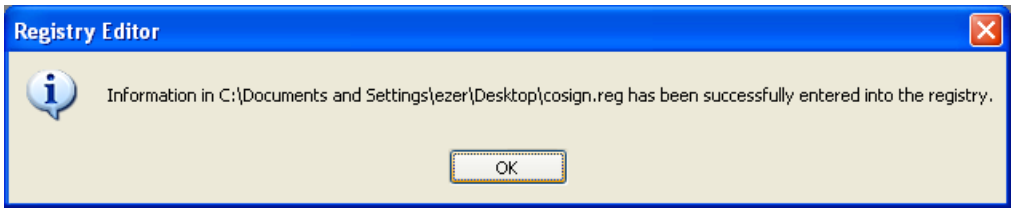
- Manually – Refer to *Distributing the DocuSign SA Configuration Manually*.
- Using Login Scripts or other distributing software – Refer to *Distributing the DocuSign SA Configuration via Login Scripts or any Distributing Software*.

Distributing the DocuSign SA Configuration Manually

> ***Note:*** You must have administrative rights on the machine in order to apply the configuration values.

To distribute the DocuSign SA configuration manually:

1. Copy the appropriate `.reg` file to the machine for which you want these settings to apply.
2. Double-click the file. A message pops up, requesting confirmation to apply the new registry values.
3. Click **Yes**, and wait for the message confirming that the operation was completed successfully.



4. Click **OK**.

> ***Note:*** Some DocuSign SA 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 DocuSign SA 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 DocuSign SA configuration files.

Distributing the DocuSign SA Configuration Using Group Policy

In an Active Directory environment, you can distribute the DocuSign SA 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.

DocuSign SA configuration values do not require a proprietary Group Policy, but are integrated in existing policies.

When opening a Group Policy in the DocuSign SA Configuration Utility, the application retrieves only the DocuSign SA-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 DocuSign SA-related definitions from the existing policy, and replaces them with the new settings. All non-DocuSign SA-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 DocuSign SA Configuration Utility to create a new policy.

Setting Admin Configuration

Admin configuration enables you to set parameters relating to the DocuSign Signature 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 DocuSign Signature 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 SA, and whether you may set AIA and CDP in the internal CA setup.

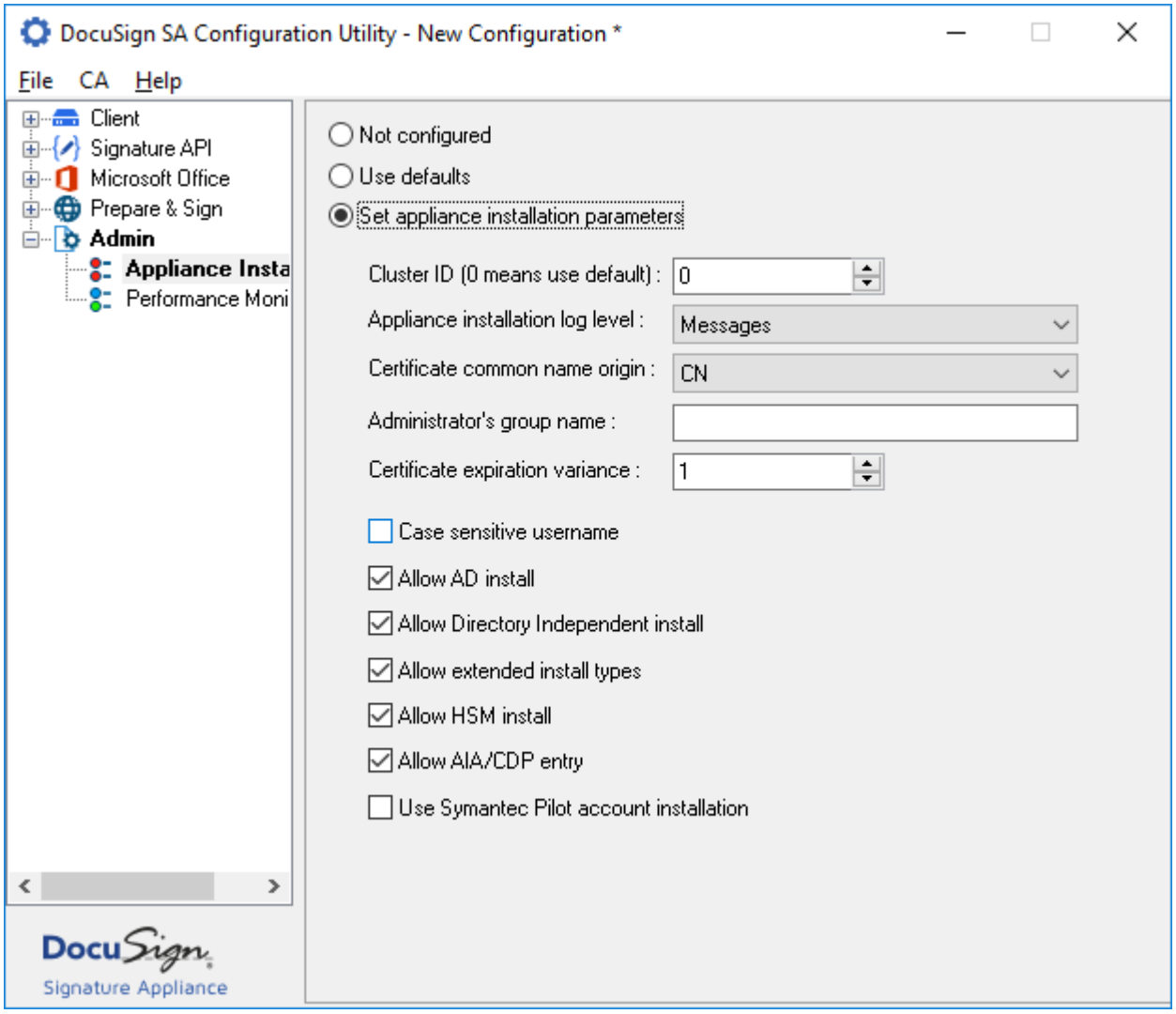


Figure 106 Configuring Admin – Appliance Installation Parameters

In the **Appliance Installation** group you can set the following Admin parameters:

DocuSign Signature Appliance related settings:

- *Cluster ID (0 means use default)* – Do not change this value unless instructed to do so by DocuSign 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 DocuSign SA 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 DocuSign SA system parameters.
- *Administrator's group name* – Specify the name of the directory service's user group that identifies authorized DocuSign SA administrators. You can select any name for this group. Make sure that all users who perform DocuSign SA 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 DocuSign SA 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 DocuSign SA installation in a Directory Independent environment.

Administrator's machine related settings:

- *Allow AD install* – Check this option to enable the administrator to install DocuSign Signature Appliance in an Active Directory environment.
- *Allow Directory Independent install* – Check this option to enable the administrator to install DocuSign Signature Appliance in a Directory independent environment.
- *Allow extended install types* – This option should always remain unchecked.
- *Allow HSM install* – Check this option to enable the administrator to install the Signature Appliance in HSM mode using the HSM client installation.
- *Allow AIA/CDP entry* – Check this option to enable the administrator to change the AIA and CDP fields in the CA setup dialog.
- *Use Symantec Pilot account installation* – Check this option to enable the administrator to communication with a Symantec Pilot account.

Admin – Performance Monitoring

Change the settings only if instructed to do so by DocuSign.

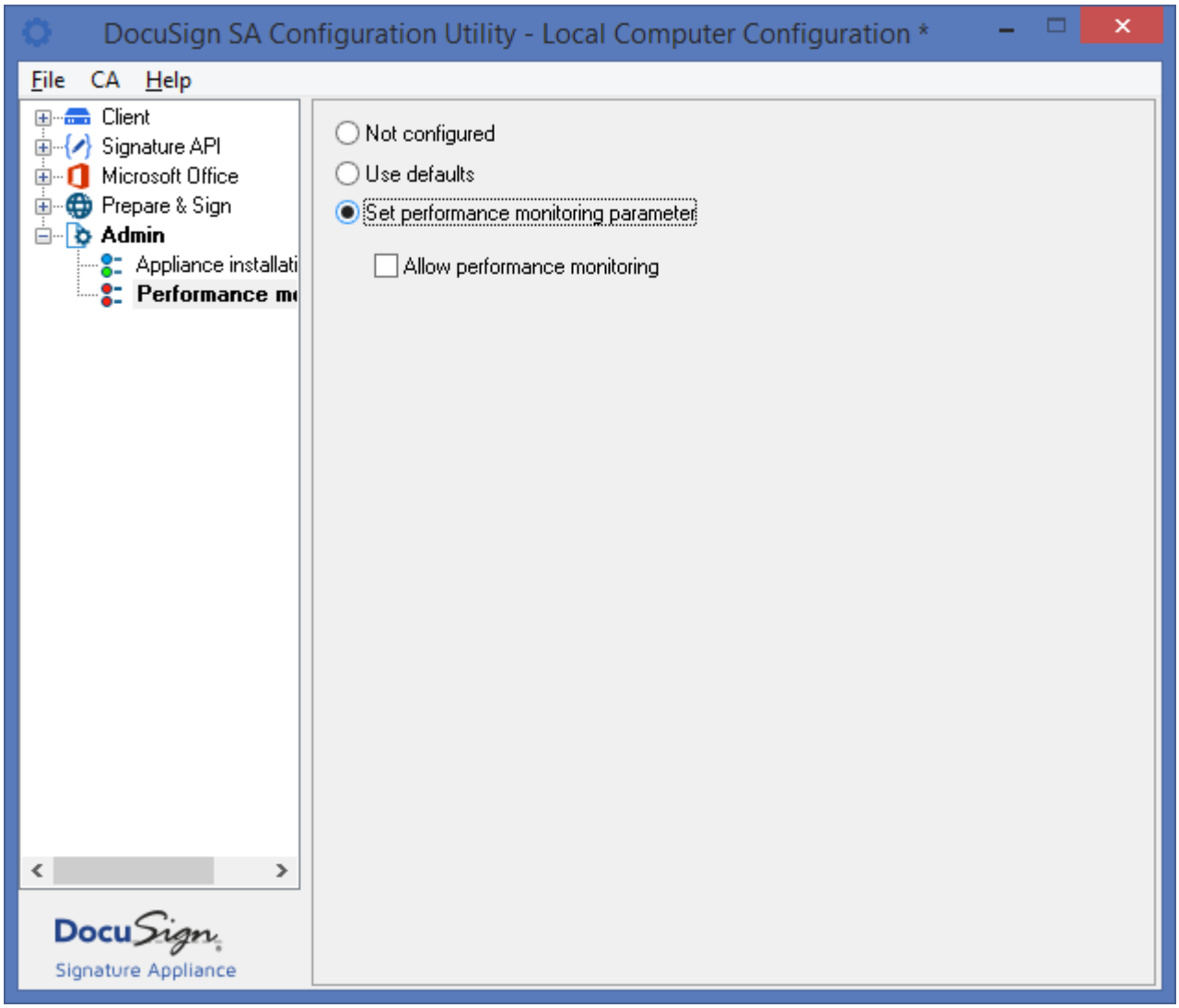


Figure 107 Configuring Admin – Performance Monitoring Parameters

Chapter 9: Troubleshooting

This chapter offers solutions to various problems you may encounter while installing or running DocuSign SA.

If you are unable to identify or solve a problem, try the DocuSign support web site at *https://support.docusign.com/en/home*

DocuSign Support information

Support web site	*https://support.docusign.com*

DocuSign Contact information

DocuSign web site:	http://www.docusign.com
DocuSign Headquarters:	221 Main St. Suite 1000 San Francisco, CA 94105

Installation Problems

This section describes various problems and error messages you may encounter during the installation process, and provides possible solutions to these problems.

DocuSign SA IP Address is Invalid

Problem: During DocuSign SA software installation, this message appears after you enter the DocuSign SA address and click **Next**.

Solution: This message indicates that DocuSign SA is not accessible. Perform the following:

- Verify that the IP address you entered is correct.
- Verify that DocuSign SA is operational.
- Check for networking problems.

Error When Setting the DocuSign SA IP Address Via the Console Interface

Problem: When setting the DocuSign SA 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 SA 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:

a. Choose the **Use DHCP** option in the DocuSign SA Console main screen.

b. Restart the DocuSign Signature Appliance.

c. Select **Ip Addr** in the DocuSign SA Console main screen to view the IP address that was allocated by the DHCP server.

d. Perform **Save**. The Appliance saves as static IP the address that was allocated by the DHCP server.

e. 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 DocuSign SA 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 DocuSign SA software installation, this message appears after you enter the DocuSign SA 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 SA to factory settings using the console, and then rerun the installation process.

Note: Since this message indicates that DocuSign SA is already installed, you may want to cancel the installation process to prevent the accidental reinstallation of DocuSign SA.

Installation Failed

Problem: The DocuSign SA 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 DocuSign SA 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 DocuSign technical support.

Error During Installation

If you get an error as part of the installation (for example, an error when an impoper license token is inserted into the Appliance), please contact DocuSign technical support for further assistance.

Progress Bar Stops Advancing

Problem: During DocuSign SA software installation, the progress bar stops advancing at the user's keys and certificate generation stage, and only one user is defined in DocuSign SA.

Solution: There may be a DNS configuration problem (in either DHCP or static IP mode). Perform the following:

- Do **not** close the DocuSign SA installation wizard.
- Modify the DNS Server IP address from the console. The progress bar will continue advancing until the installation is completed.

DocuSign Signature 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 DocuSign Signature Appliance failed to join the domain due to network configuration problems.

Solution: Check for network setting such as DNS IP on the DocuSign SA 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 DocuSign Signature Appliance IP using the `-a` option. You should get a reply with the appliance full DNS name.

Error when communicating with DocuSign CA or DocuSign TSCP CA

Problem: When an RA certificate is sent by DocuSign in reply to an RA certificate renewal request, the DSA communicates with DocuSign CA or DocuSign TSCP CA. During the operation, the administrator gets an error such as *Uploading Certificate reply failed with status code 10240. Please refer to…*

Such a problem may also occur during normal operation of the Appliance.

Cause: The DocuSign Signature Appliance failed to communicate with DocuSign CA or DocuSign TSCP CA.

Solution: Check the communication network between the DSA and DocuSign CA or DocuSign TSCP CA. Perhaps a proxy is defined inside the organization and you are failing to communicate with the external service through the proxy.
Or perphas the organization's firewall is not properly configured to forward the requested communication to DocuSign CA or DocuSign TSCP CA.

High Availability/Load Balancing – Alternate Installation

Problem: After completing the installation of an alternate DocuSign SA, the following message appears in the subscribed alternate: "The snapshot for this publication has become obsolete".

Cause: You did not restart the primary DocuSign Signature Appliance before starting the alternate installation.

Solution:

1. Unsubscribe the alternate appliance.
2. Restore the alternate to factory settings.
3. Restart the primary appliance (hardware restart).
4. Re-install the alternate appliance.

DocuSign Signature Appliance Problems

DocuSign Signature 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: *DocuSign SA is now starting, please wait*. Even after restarting DocuSign SA several times the same message continues to display.

- **Solution 2:** Follow the instructions in *Restoring the DocuSign Signature Appliance after an Internal Hard Disk Failure*. It is recommended to consult with DocuSign technical support before carrying out the instructions.

Console Problems

The console provides messages and alerts for the following problems (refer to *DocuSign SA 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 DocuSign SA license limit` – Contact DocuSign to obtain a larger license.

- `DocuSign Signature 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 DocuSign Signature Appliance has passed the license limit. Warning <num> of 5, system will shutdown!` – Either obtain a new license MiniKey from DocuSign, or remove users from the scope of DocuSign SA 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 DocuSign SA 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 SA User Guide*.

Cannot See Any Certificates in Store

Problem: You cannot see any certificates in your Microsoft Personal certificates store.

Solution: Perform the following:

1. Restart the machine and try again.
2. Verify the following:
   - You are logged in to the same domain as DocuSign SA. 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 DocuSign SA IP address or try to connect to DocuSign SA using telnet to port 443.
   - Your user account is defined in the directory that was defined as the AD users container during DocuSign SA 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 **DocuSign SA Configuration Utility** to setup the DocuSign Signature Appliance IP address (refer to the Client – Appliances section in the DocuSign SA Configuration Utility chapter of the *DocuSign SA User Guide*).

Administrative Problems

This section describes various problems and error messages you may encounter while managing DocuSign SA, and provides possible solutions to these problems.

DocuSign SA System Parameters Do Not Appear in the DocuSign SA Administration MMC

Problem: You do not see any DocuSign SA system parameters in the DocuSign SA Administration MMC.

Solution: In order to perform administrative operations using the DocuSign SA Administration MMC, you must be a member of the DocuSign SA 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 DocuSign SA Console (refer to *Chapter 6: Using the DocuSign SA Console*).

All DocuSign SA Administration MMC Operations Fail

Problem: Any operation you attempt to perform in the DocuSign SA Administration MMC fails.

Solution: Refer to *DocuSign SA System Parameters Do Not Appear in the DocuSign SA Administration MMC*.

DocuSign SA Does Not Respond

Problem: You cannot access DocuSign SA through the DocuSign SA 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 SA to turn itself off after two hours. Insert the correct license MiniKey and restart DocuSign SA.
- A tamper event occurred, and the Tamper LED is blinking. Reset the Tamper mechanism from the console (refer to *Resetting the Tamper Mechanism*).
- DocuSign SA 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 SA begins working.
- The DocuSign SA users OU was modified. Verify that the DocuSign SA users OU was not modified, and it is the same as was entered during DocuSign SA installation.

If none of the above is applicable, access the console and select the **Status** tab (refer to *Displaying DocuSign Signature Appliance Status*). Check the appliance information for the DocuSign SA Service Status parameter, as follows:

- If the DocuSign SA Service Status is **Running**, check for a network problem between DocuSign SA and the clients.
- If the DocuSign SA Service Status is **Stopped**, restart DocuSign SA and then recheck the DocuSign SA Service Status. If the DocuSign SA Service Status is still **Stopped**, contact DocuSign technical support.

- If the DocuSign SA Service Status is neither **Running** nor **Stopped**, first check to see whether there is a networking problem (ping the DocuSign SA IP address). If this is not the problem, contact DocuSign technical support.

New Users Do Not Receive Certificates

Problem: When you add new users to the system, DocuSign SA does not assign the users certificates.

Solution: Verify that the number of users does not exceed the DocuSign SA 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 as the values of the **Users** parameter in the console's **Status** tab (refer to *Displaying DocuSign Signature Appliance Status*).

If there are too many users defined in the Users OU, perform one of the following actions:

- Request a new license from DocuSign.
- Delete unnecessary users.
- Move some of the users to another OU.

Then perform Sync with Directory from the DocuSign SA Administration MMC (refer to *Synchronizing DocuSign SA 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 DocuSign SA database. Download the Audit log. If this is the problem, the message `DocuSign Signature Appliance reach license limit, please upgrade your DocuSign SA license` appears. In this case, perform Sync with Active Directory from the DocuSign SA 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 SA 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 DocuSign Signature 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 DocuSign SA Operation Fails

Problem: When attempting to back up the DocuSign Signature Appliance using the `getbackup.exe` utility or the DocuSign Signature Appliance management console, the backup process fails. The administrator has full administrative privileges on the MS Active Directory.

Cause 1: DocuSign SA administrative tasks can be performed only by a user who is himself a member of the DocuSign SA administrators group (and not a member of a group that is member of the DocuSign SA administrators group).

Solution 1: Check the name of the DocuSign SA administrators group on the DocuSign Signature Appliance console and make sure you are yourself a member of that group.
It is also possible to use the DocuSign SA built-in administrator.

Cause 2: On the debug log you will see that the backup failed because it failed to copy the DocuSign SA internal CA CRL file.

Solution 2: Perform a hardware restart.

Appendix A: DocuSign SA Installation with Reduced Privileges

This appendix describes how to perform DocuSign SA installation in an Active Directory environment with reduced permissions.

Overview

When the DocuSign Signature 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 SA.

DocuSign Signature Appliance installation is performed using the *DocuSign Signature Appliance Management* utility and is described in detail in *Chapter 3: Installing DocuSign SA*.

There are cases where the DocuSign Signature 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.

DocuSign SA Client enables administrators with restricted permissions to install the DocuSign Signature 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 SA.

This appendix describes the differences between a regular DocuSign SA installation and a DocuSign SA installation with reduced privileges. It includes the following sections:

- *Regular DocuSign SA Installation* – This section describes a regular DocuSign Signature Appliance installation, with a focus on the Active Directory operations performed by the installation, and the functional purpose of each Active Directory operation.
- *DocuSign SA Installation with Reduced Privileges* – This section describes the reduced DocuSign Signature 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 DocuSign SA Installation

The following sections list all the operations carried out during DocuSign Signature Appliance installation that require Enterprise admins or Domain admins permissions.

Creating a New Computer Account for the DocuSign Signature Appliance

The installation creates a new computer account for the DocuSign Signature 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 DocuSign Signature Appliance to MS Domain

In order to install DocuSign SA 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 DocuSign SA IP address) that enables the DocuSign SA Clients to connect to the DocuSign Signature Appliance. This object is located in **Active Directory Sites and Services** → **Services** → **Net Services.**

The DocuSign Signature Appliance computer account is granted read and write access rights so that the DocuSign Signature Appliance can update SCP information.

DocuSign SA User Synchronization

During normal operation, the DocuSign Signature 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 DocuSign Signature Appliance to enable querying the deleted user objects.

Updating the userCertificate Attribute for Users

DocuSign SA 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 DocuSign SA 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 DocuSign Signature Appliance.

DocuSign SA CA Root Certificate Information

AIA (Authority Information Access) and CA objects that contain the DocuSign SA published Certificate Authority root certificate are updated by the DocuSign Signature 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 DocuSign Signature Appliance computer account so that the appliance can publish and update CA objects.

DocuSign SA CA CDP (Certificate Distribution Point)

The DocuSign SA CA CDP (CRL Distribution Point) contains the updated DocuSign SA's 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 DocuSign Signature Appliance computer account so that the appliance can publish and update new CRLs.

DocuSign SA Installation with Reduced Privileges

During the DocuSign SA 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 DocuSign SA computer to the domain as a preliminary action to be taken before installing with reduced privileges.
- Install DocuSign SA in a reduced-privileges environment.
- Complement the DocuSign SA installation with the DocuSign SA capabilities that were described in *Regular DocuSign SA Installation*.

Preliminary Action – Adding the DocuSign SA Computer to the Domain

Prior to running the DocuSign SA installation, add the DocuSign SA 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 DocuSign SA serial number (refer to *Displaying DocuSign Signature Appliance 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 DocuSign SA installation should be the above user or a user who is a member of the assigned group.

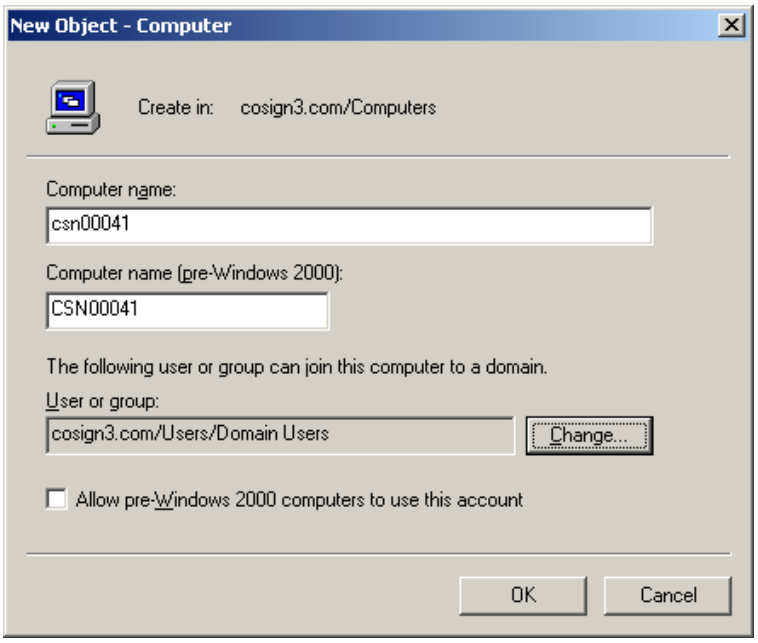


Figure 108 Adding the DocuSign SA Computer to the Domain

Installing DocuSign SA in a Reduced Privileges Environment

After adding the DocuSign SA computer to the domain, activate the DocuSign Signature Appliance Management and install the DocuSign Signature Appliance according to the following guidelines:

1. In the *User Setup* window provide the username and password for an account with permission to join the DocuSign SA machine to the domain.
2. In the *Directory Setup* window set the **DocuSign SA Container** field with the full OU (or container) path of the DocuSign SA computer account that was generated in the preliminary stage.
3. 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.

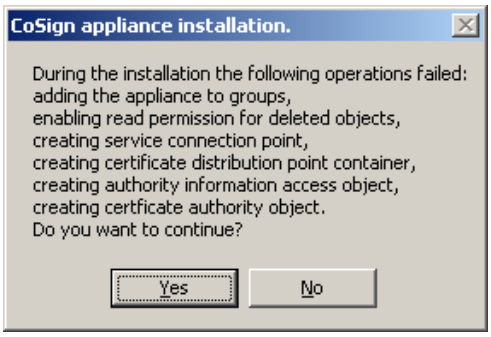


Figure 109 Installation Failure Message

4. 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 DocuSign SA 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 DocuSign SA capabilities after installing with reduced privileges.

> ***Note:*** After you update any of the objects in the Active Directory, restart the DocuSign Signature Appliance.

Joining the DocuSign Signature Appliance to the MS Domain

For DocuSign SA to work, it is mandatory that the user specified in the *User Setup* window has permission to join the DocuSign Signature Appliance to the Domain.

Administrating DocuSign SA after the installation

To administrate DocuSign SA after the installation, use the *DocuSign SA Configuration Utility* (described in *Chapter 8: DocuSign SA 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 SA using the DocuSign SA built-in administrator.

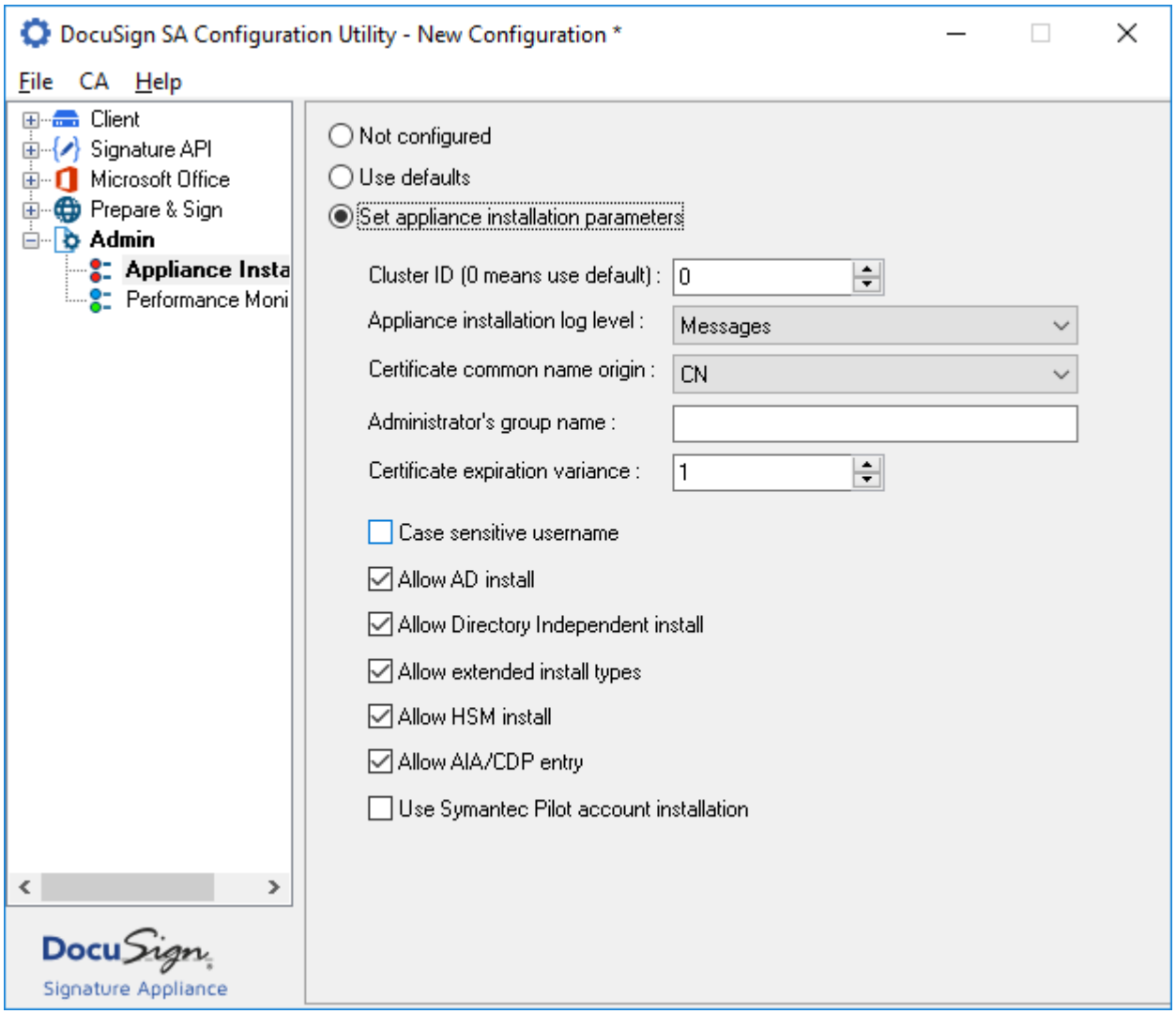


Figure 110 Setting the Administrator's Group Name

Creating a Services Connection Point (SCP)

Failure to create an SCP prevents the DocuSign Signature Appliance from publishing its binding information, thus preventing DocuSign SA clients from locating the DocuSign Signature Appliance. Once the DocuSign SA 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 DocuSign SA Client Configuration utility (refer to *Distributing DocuSign SA Information through the SCP*). However, this option is limited for the following reasons:

- The client is never updated with the current status of the DocuSign Signature Appliance activity. This causes long delays when attempting to connect to an inactive appliance.
- Any update of information, such as the DocuSign Signature Appliance's IP address, involves a manual update of all DocuSign SA clients.

DocuSign SA 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 DocuSign SA 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 DocuSign Signature Appliance (refer to *Synchronizing DocuSign SA with the Directory Service*).

Updating the userCertificate Attribute for Users

Failure to assign the DocuSign SA 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 DocuSign SA computer as a member of the *Cert Publishers* group.
- Grant the DocuSign SA computer write access to the relevant users.
- Publish the user certificate manually, or refrain from publishing users' certificates.
- Note that DocuSign SA does not update the certificate attribute of the user by default.

Appliance's CA Root Certificate Information

Failure to create the AIA prevents the DocuSign SA server from automatically publishing its ROOT certificate. Since the DocuSign SA 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 SA Client* for more information.
- During the installation of the DocuSign Signature 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.

Appliance's CA CDP (Certificate Distribution Point)

Failure to create a CDP prevents the DocuSign Signature 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 DocuSign SA 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 DocuSign Signature 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 DocuSign Signature Appliance the proper rights to update this object.

Appendix B: Centralized DocuSign SA Client Installation

The DocuSign SA 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 DocuSign SA client in a large scale organization using Microsoft SCCM (System Center Configuration Management).

Note: Starting from DocuSign SA client version 8.5, the installation is based on a single client installation file.
The required .msi files for the following process are provided in the DocuSign SA CD.

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 DocuSign SA client on all relevant workstations without user intervention, resulting in a smooth deployment of the DocuSign SA 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/.

Automatic deployment in a Microsoft Active Directory can be performed as follows:

1. Place the contents of the **MSI** directory of the DocuSign SA 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.
2. Define a Task Sequence in Microsoft SCCM. When the task sequence is advertised, the relevant workstations will install the DocuSign SA client software. For more information, refer to *Defining and Advertising a DocuSign SA Client Task Sequence*.

DocuSign SA Installation Components

The following table lists the components of the DocuSign SA Client installation, and their location in the DocuSign SA CD. These files are used to define which DocuSign SA Client software packages SCCM will install.

Table 2 DocuSign SA Client Installation Components

Installation Files for 64-bit Operating Systems	Location
DocuSign SA Client64.msi	CDRom\MSI
DocuSign CryptoKit Basic64.msi	CDRom\MSI
DocuSign Signature API64.msi	CDRom\MSI
PDFCreator-2_5_2_5233-Setup-arx-cosign_x64.msi (Optional)	CDRom\MSI
DocuSign Office Signatures64.msi (Optional)	CDRom\MSI

Note: If you install an optional PDF Printer package (PDFCreator-2_5_2_5233-Setup-arx-cosign_x64.msi), you need to also deploy and install the registry file *NewPdfCreator.reg* as described in *Defining and Advertising a DocuSign SA Client Task Sequence*.

Defining and Advertising a DocuSign SA Client Task Sequence

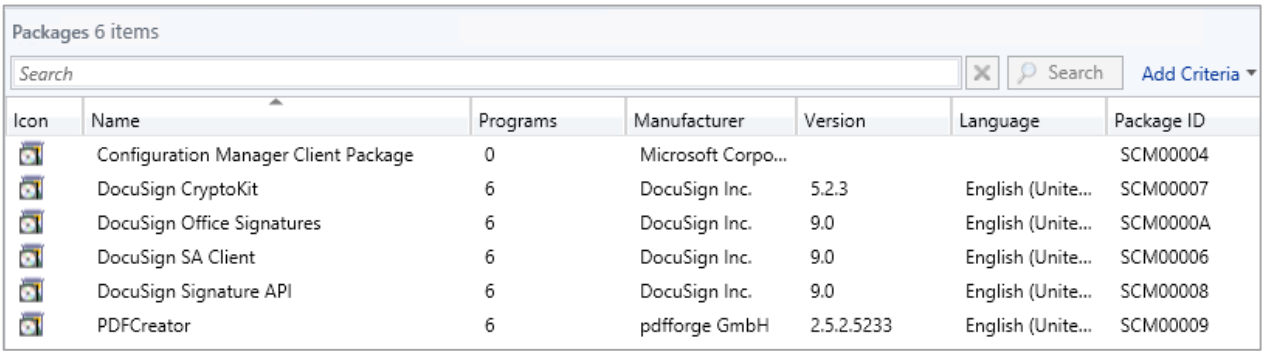
This section describes in detail how to define a Microsoft SCCM Task Sequence for DocuSign SA client installation, and how to advertise the Task Sequence so it performs automatic mass DocuSign SA client installation in large scale DocuSign SA client deployments.

Step 1: Define DocuSign SA Packages

To define DocuSign SA packages:

1. Open the SCCM Configuration Manager Console.
2. Navigate to **Software Library > Overview > Application Management > Packages**.
3. Select **Home > Create Package from Definition** to add as software packages each of the following software components (.MSI files) that you had placed in the shared location:
   - DocuSign SA Client64.msi
   - DocuSign CryptoKit Basic64.msi
   - DocuSign Signature API64.msi
   - PDFCreator-2_5_2_5233-Setup-arx-cosign_x64.msi (if required)
   - DocuSign Office Signatures64.msi (if required)

   The full list of packages will look similar to the following:



Icon	Name	Programs	Manufacturer	Version	Language	Package ID
	Configuration Manager Client Package	0	Microsoft Corpo...			SCM00004
	DocuSign CryptoKit	6	DocuSign Inc.	5.2.3	English (Unite...	SCM00007
	DocuSign Office Signatures	6	DocuSign Inc.	9.0	English (Unite...	SCM0000A
	DocuSign SA Client	6	DocuSign Inc.	9.0	English (Unite...	SCM00006
	DocuSign Signature API	6	DocuSign Inc.	9.0	English (Unite...	SCM00008
	PDFCreator	6	pdfforge GmbH	2.5.2.5233	English (Unite...	SCM00009

Figure 111 Defining the DocuSign SA Packages

Step 2: Create a Task Sequence

To create a task sequence:

1. Navigate to **Software > Overview > Operating Systems > Task Sequences**.



Figure 112 Task Sequences Window

2. Select **Home > New custom task sequence**. The New Task Sequence Wizard is launched.

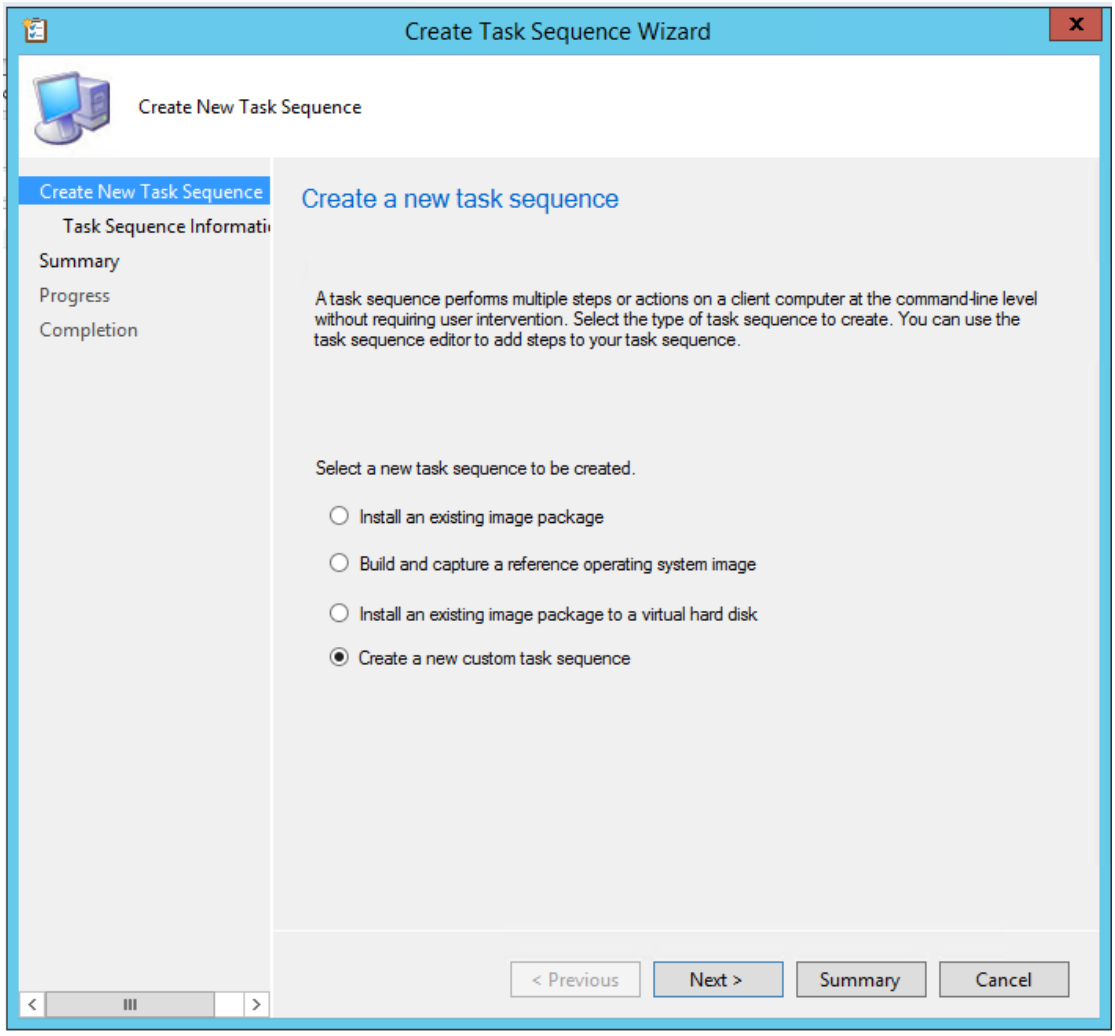


Figure 113 New Task Sequence Wizard

3. Select **Create a new custom task sequence**.

4. Give the new task sequence a name. It is recommended to give it the same name as the installed DocuSign SA Client version.



Figure 114 Name of Task Sequence

5. Right-click the newly created Task Sequence and select **Edit.** The Task Sequence Editor window appears.

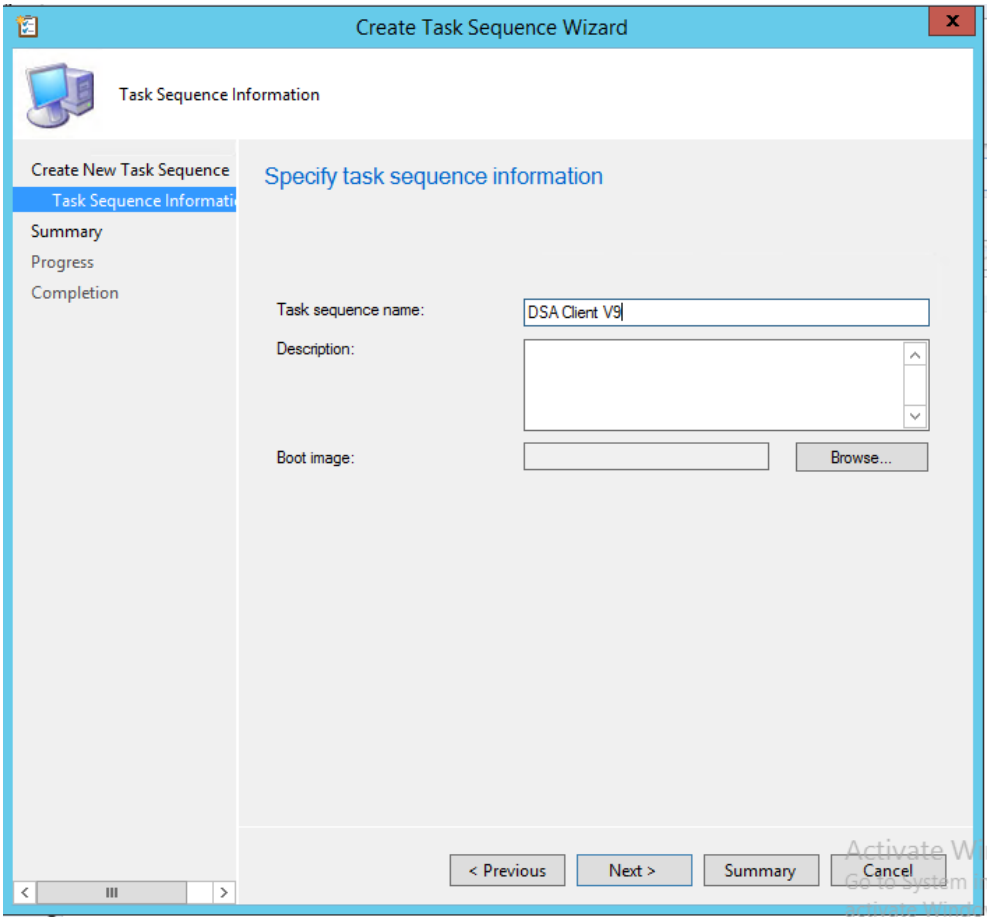


Figure 115 Task Sequence Editor window

6. Install the DocuSign SA Client as follows:
   a. Select **Add > Software > Install Package**.

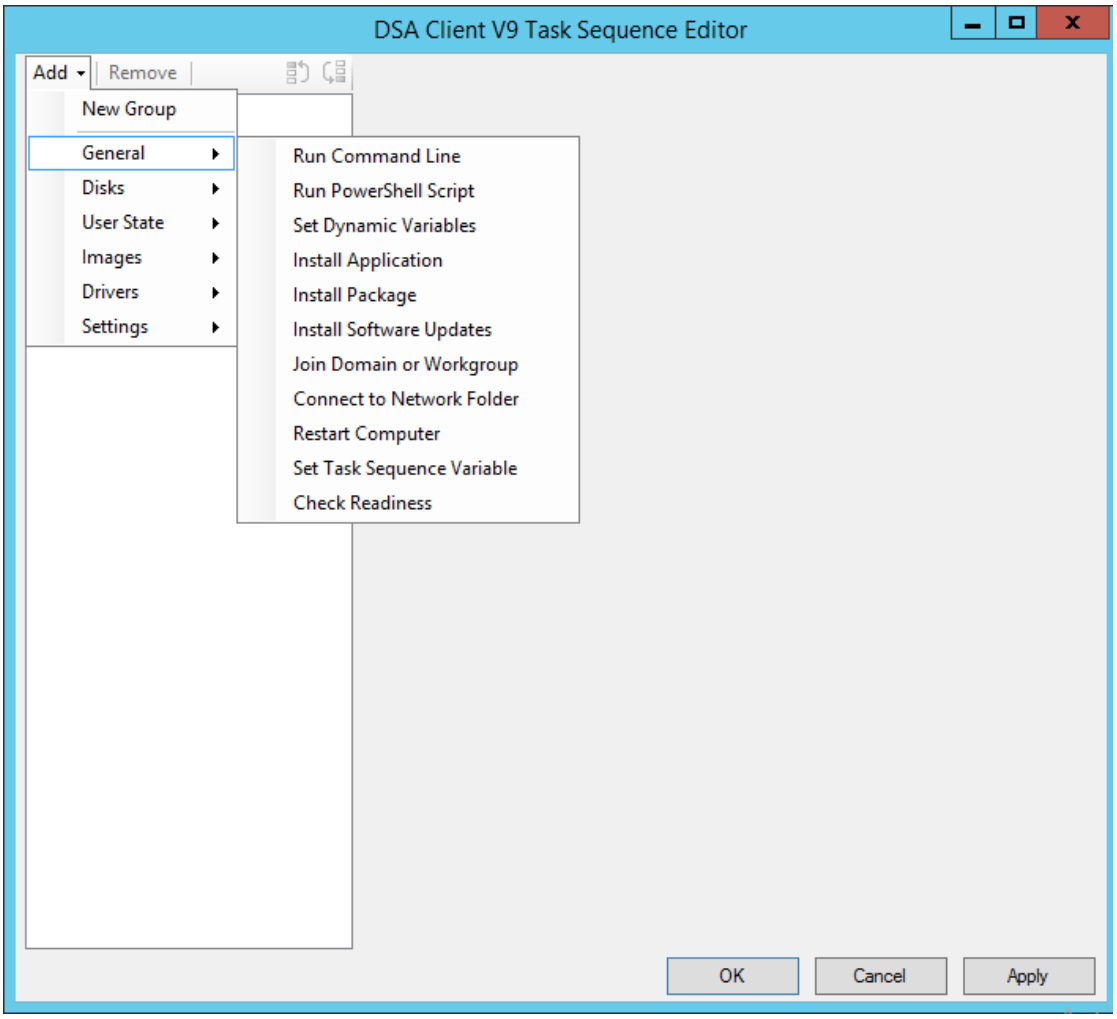


Figure 116 Selecting to Install Software

   b. In the **Name** field, enter a meaningful name for the software.
   c. Click **Browse** to select the relevant package.
   d. Verify that **Per-system unattended** is selected in the **Program** field.

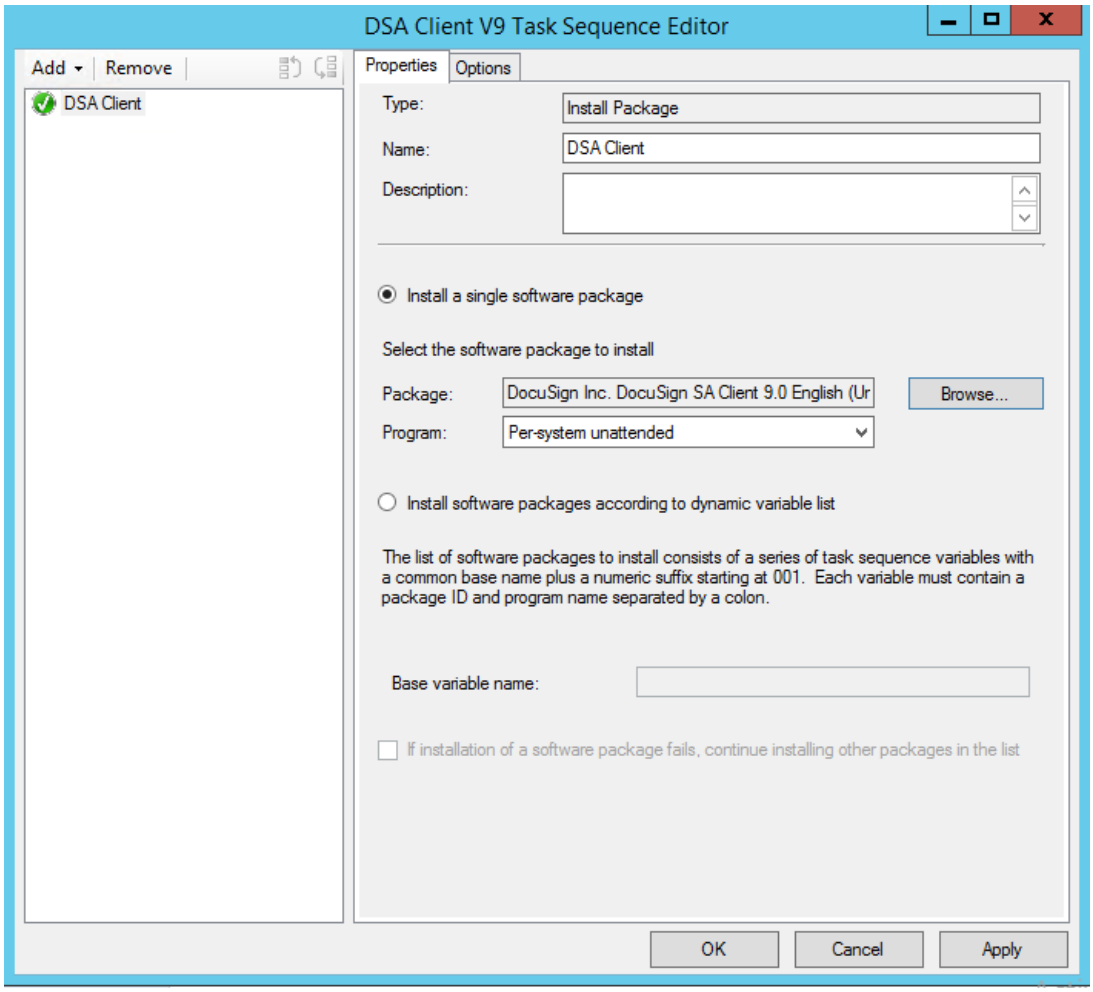


Figure 117 Installing a Package as Software

e. Click **Apply**.

7. Install DocuSign CryptoKit as follows:
   a. Navigate to **Add > Software > Install Package**.
   b. In the **Name** field, enter a meaningful name for the software.
   c. Click **Browse** to select the relevant package.
   d. Verify that **Per-system unattended** is selected in the **Program** field
   e. Click **Apply**.
8. Install the DocuSign SA Signature API as follows:
   a. Select **Add > Software > Install Package**.
   b. In the **Name** field, enter a meaningful name for the software.
   c. Click **Browse** to select the relevant package.

d. Verify that **Per-system unattended** is selected in the **Program** field.

e. Click **Apply**.

9. Optionally install the DocuSign SA Office Signatures as follows:

a. Select **Add > Software > Install Package**.

b. In the **Name** field, enter a meaningful name for the software.

c. Click **Browse** to select the relevant package.

d. Verify that **Per-system unattended** is selected in the **Program** field.

e. Click **Apply**.

10. Optionally install the DocuSign SA Printer as follows:

a. Select **Add > Software > Install Package**.

b. In the **Name** field, enter a meaningful name for the software.

c. Click **Browse** to select *PDFCreator-2_5_2_5233-Setup-arx-cosign_x64.msi*.

d. Verify that **Per-system unattended** is selected in the **Program** field.

e. Click **Apply**.

f. Install the registry file that binds the printer to the *Prepare&Sign* utility, as described in the following step.

> ***Note***: The displayed printer name in this mode of installation is "PDF Creator" and not "DocuSign Signature Appliance Printer Driver". In addition, the package is not installed in the **`Program files\arx\PDFCreator`** location but in the **`Program files\PDFCreator`** location.

11. If you installed the DocuSign SA Printer (as described in the previous step), you must install the registry file that binds the printer to the *Prepare&Sign* utility, as follows:

a. Navigate to **Add** > **General** > **Run Command Line**.

b. In the **Name** field, enter a meaningful name.

c. In the **Command line** field enter the following text:

```
regedit /s "{share}\NewPdfcreator.reg"
```

where **`{share}`** is the location of the shared disk.

d. Click **Apply**.

12. Click **OK**.

Step 3: Advertise the Task Sequence

To advertise the task sequence:

1. Navigate to **Software > Overview > Operating Systems > Task Sequences**.

2. Select the DocuSign SA Client task sequence and click the **Deploy** button from the home menu.

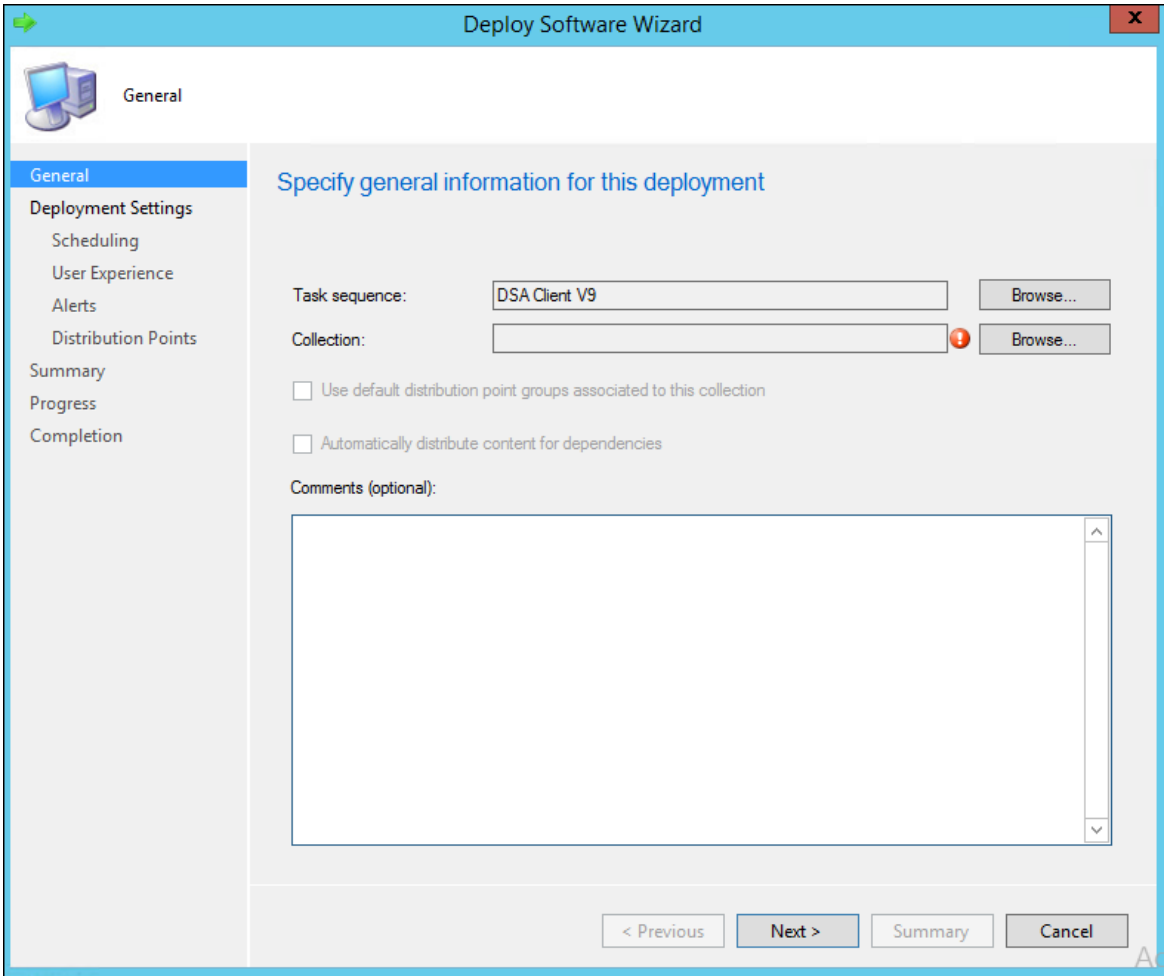


Figure 118 New Advertisement Wizard

3. Give the new task advertisement a name. It is recommended to give it the same name as the task.
4. Click **Browse** adjacent to the **Task Sequence** field to select the task sequence
5. Click **Browse** adjacent to the **Collection** field to specify on which workstations to install the packages in the task sequence.
6. Click **Next**, and in the Schedule window set the date and time of the installation.
7. Click **Next** in all subsequent wizard windows, and click **Finish** in the final window.

Appendix C: Requirements for Accessing External Resources

In some cases, depending on the installation or configuration of the DocuSign Signature Appliance, the DocuSign Signature Appliance needs to access external network resources. In those cases, organizational firewalls will be required to allow that access.

This appendix provides information for enabling access to external network resources. The information includes the DNS name of the services and their ports.

If the organization accesses external network resources using a proxy, the proxy should be configured to allow the required communication. For more information on how to configure the proxy parameters in the DocuSign Signature Appliance, refer to *Advanced Settings* in the *Installing the DocuSign Signature Appliance Software* chapter as well as to *Advanced Parameters* in *Changing DocuSign SA System Parameters*.

Automated External CA – DocuSign CA or DocuSign TSCP CA

http://tc-ws-tscp.dsf.docusign.net – for both a Production account and a Demo account

Automated External CA – Comodo

https://secure.comodo.net

http://crt.comodoca.com or http://crt.comodoca.com:8080

http://crt.usertrust.com or http://crt.usertrust.com:8080

In addition, the following resources need to be accessible through either port 80 or 8080:

http://crl.comodoca.com/COMODORSAExtendedValidationSecureServerCA.crl

http://crl.comodoca.com/COMODORSACertificationAuthority.crl

http://crl.usertrust.com/AddTrustExternalCARoot.crl

http://ocsp.usertrust.com

http://ocsp.comodoca.com

Automated External CA – Symantec

https://pki-ws.symauth.com/pki-ws – for a Production account

https://ptnr-pki-ws.bbtest.net/pki-ws – for a Pilot account

General CRL/AIA/OCSP access for a Certificate Authority

As part of the certificate validation process, external resources need to be accessed. If access is denied, services may not work properly.
The following cases summarize the situations where External Certificate Authorities need to be accessed:

DSA is deployed in an LDAP environment with SSL/TLS

As part of the SSL/TLS communication with the LDAP server, the DSA needs to validate the certificate of the LDAP Server. The CA that authorized the LDAP Server's certificate will be accessed as part of the validation process.
The exact URLs that need to be accessed can be viewed in the *CRL Distribution Point* or *Authority Information Access* attributes in the TLS/SSL Server certificates of the LDAP Server.

Certificate of IDP (Identity Provider) that produces the SAML Tokens

If the DocuSign Signature Appliance is configured to use SAML tickets for user authentication, the DSA needs to validate the certificate of the IDP (SAML generation certificate). The CA that authorized the SAML Server's certificate will be accessed as part of the validation process.
The exact URLs that need to be accessed can be viewed in the *CRL Distribution Point* or *Authority Information Access* attributes in the TLS/SSL Server certificates of the LDAP Server.

Certificate validation performed as part of the DocuSign SA REST/SOAP

If the DocuSign Signature Appliance is configured to use SOAP or REST interfaces, the Signature Validation API may be called.
If an external CA issued the signing certificate, the CA will be accessed as part of the validation process.
The exact URLs that need to be accessed can be viewed in the *CRL Distribution Point* or *Authority Information Access* attributes in the TLS/SSL Server certificates of the LDAP Server.

Appendix D: WinPcap Copyright Notice

The WinPcap software is used as part of the DocuSign Signature Appliance. The following presents the WinPcap copyright notice.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.
This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
This product includes software developed by Yen Yen Lim and North Dakota State University.

Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 1995, 1996, 1997 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the Kungliga Tekniska Högskolan and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1997 Yen Yen Lim and North Dakota State University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by Yen Yen Lim and North Dakota State University"
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.
THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1996 Juniper Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution. The name of Juniper Networks may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions Copyright (c) 2001 Daniel Hartmeier All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright 1989 by Carnegie Mellon.

Permission to use, copy, modify, and distribute this program for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting

documentation, the name of Carnegie Mellon not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Carnegie Mellon and Stanford University. Carnegie Mellon makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Index

—A—

Accepting Relying Parties Tickets, 164
Accessing DocuSign SA, troubleshooting, 248
Accessing external resources, 266
  accessing external CAs, 267
  Comodo, 266
  DocuSign CA, 266
  DocuSign TSCP CA, 266
  Symantec, 266
Activating a user, 22
Active Directory. *See* Microsoft Active Directory
Add Certificate to CRL, 145
Add Digital Signature checkbox disabled, 247
Additional Radius IPs (CC Mode), 163
ADFS, 25
Administrative problems, troubleshooting, 248
AIA Location Settings, 144
AIA Publication Location, 144
Allow Get Backup Anonymously, 159
Allow Only Built-in DocuSign SA Admin, 150
Alternate DocuSign Signature Appliance
  data replication management, 223
  installing, 218
  installing hardware, 218
  installing software, 218
  managing, 222
  overview, 215
  re-initializing, 224
  resubscribing, 228
  setting as primary appliance, 224
  unsubscribing, 224
  viewing replication status, 223
Alternate Extended Auth Mode, 161
Alternate Radius Server Address, 162
Alternate Radius Server port, 162
Appliance
  configuring installation parameters, 240
  configuring performance monitoring parameters, 242
  configuring the signing operation using the DocuSign SA Configuration Utility, 240
  connecting DocuSign SA Enterprise HW v8.0, 38
  connecting DocuSign SA FIPS HW v8.0, 33
  DocuSign SA Enterprise back panel, 38
  DocuSign SA Enterprise front panel, 38
  DocuSign SA FIPS HW v8.0 back panel, 34
  DocuSign SA FIPS HW v8.0 front panel, 34
  managing, 114
  not in factory settings mode, error message, 244
  restarting appliance, 117
  restarting services, 117
  restore operation fails, 249
  restoring in Active Directory, 168
  restoring in Directory Independent environment, 169
  restoring in LDAP environment, 169
  restoring, overview, 167
  synchronizing with directory service, 136
  viewing information in web-based Console, 208
Appliance Administrator Group, 149
Appliance Debug Level, 157
Appliance RA Certificate serial number, 147
Applications that work with DocuSign SA, 12
Architecture, 16
Audit log
  command line utility, 187
  downloading, 123
  enabling user counters, 155
  entries ID and descriptions, 124
  Maximum number of rows, 155
  reporting client application name, 155
  reporting signature events, 154, 155
  storage period, 155
Audit log storage period, 155
AuditLogDownloadUtility, 191
Authenticating
  data, requirements, 11
  users in DocuSign SA, 17
Authentication key renewal, automatic external CA, 84, 128
Authentication key renewal, ChosenSecurity CA, 130
Authentication methods, 17
Authentication, extended authentication mechanisms, 17, 113
Automatic Deletion of Users, 148
Automatic deployment of DocuSign SA client
  in Active Directory, 258
  overview, 258
Automatic external CA
  renewing authentication key, 84, 128

—B—

Back panel
  DocuSign SA Enterprise, 38
  DocuSign SA FIPS HW v8.0, 34
Backing up the database, 116
Backup
  backup fails, troubleshooting, 250

command line utility, 186
operation, 116
restoring appliance from, 167
Backup minikey, copying, 201
Batch scripts, 186

—C—

CA
adding, 138, 140
disabling, 143
setting parameters, 143
CA Account Name, 147
CA Cert Hash Algorithm, 145
CA Range, 146
CA Service Connection Point, 146, 147
Case Sensitive Username, 159
CD
installation files, 105
CDP location settings, 144
Central storage of keys, 17
Centralized installation of DocuSign SA client, 258
Certificate Common Name, 146, 150
Certificate Expiration Variance, 145
Certificate Refresh Timer, 152
Certificate Refresh Window, 145
Certificate Revocation List (CRL)
CRL publishing frequency, 145
downloading to a file, 234
Certificate Validity Period, 144
Certificate's country, 146
Certificate's organization, 146
Certificate's organizational unit, 146
Certificates
automatic external CA mode, 19
certificate validity period, 144
creating for each computer, 149
DocuSign SA FIPS HW v8.0 certificates compliance, 37
expiration variance, 145
groups, 149
internal CA, installing, 69
manual external CA mode, 19
none in store, 247
parameters, setting, 152
publishing, 150
refresh timer, 152
refresh window, 145
refreshing, 141
ROOT, adding to trusted CA list, 112
ROOT, installing, 112
setting certificate's country, 146
setting certificate's organization, 146
setting certificate's organizational unit, 146
setting common name, 146, 150
troubleshooting, 249
ChosenSecurity external CA
renewing authentication key, 130
setting up, 80
uploading CA information, 82, 85
Client
deployment
deployment options, 103
introduction, 103
on end-user machine, 103
on terminal server, 103
on Web server, 104
overview, 103
installing, 104, *See* Client installation
installing centrally, 258
setting security parameters, 152
software components, 105
supported operating systems, 103
troubleshooting, 247
uninstalling, 108
Client installation
automatic centralized deployment, 108
centralized installation, 258
client MSI files, 258
installing from CD, 106
overview, 104
prerequisites, 106
Clients Inactivity Timeout, 158
Cloud Monitoring, 160
Cloud Monitoring Reporting Type, 160
Cloud Monitoring timer, 161
Cloud Site ID, 160
Command line utilities
AuditLogDownloadUtility, 191
GetBackup, 186
GetEvt, 187
getServerReport, 190
installing, 186
overview, 186
RestartServer.exe, 188
SetSCP, 190
Switch2Prim, 189
Common Criteria EAL4+, 20
certificate enrollment, 23
DocuSign SA installation procedure, 66
Radius server, 21
signature key generation, 23
user activation, 22
Common Criteria Mode, 160
Radius callback list, 163
Common Criteria Type, 160
Configuring
DocuSign SA, using the Configuration Utility, 230
Console

error messages, 246
troubleshooting, 246
Console, web-based
accessing, 194
checking security information match, 205
copying backup Minikey, 201
downloading server logs, 207
enabling DHCP, 197
resetting tamper, 199
restarting appliance, 199
restoring factory settings, 200
setting appliance IP address, 196
setting DocuSign SA time, 197
shutting down DocuSign SA, 199
touch screen, using, 212
uploading software, 206
using, 194
viewing DocuSign SA information, 208
Contact Name, 164
CORS domain for REST API, 159
CPS Object ID, 145
CPS URI, 145
Create Computer Keys, 149
Create Group Keys, 149
Create User Key Mode, 151
CRL Publication Location, 144
CRL Publishing Frequency, 145
CRL Validity Period, 145

—D—

Data authentication systems, 11
Data flow in DocuSign SA, 16
Data replication management
accessing, 223
re-initializing an alternate appliance, 224
unsubscribing an alternate appliance, 224
viewing replication status, 223
Database, backing up, 116
Date, setting in web-based Console, 197
Debug
level, 157
log, downloading, 123
Default Radius password length, 162
Delete expired users by window, 152
DHCP
enabling in web-based Console, 197
Digital signatures, prompting for signature, 154
Directory Independent environment
Directory Independent Users Management utility, 170
installing DocuSign SA software, 60
overview, 18
password policy, 155
restoring appliance, 169
Directory Server Search Base, 150
Directory Synchronization Timer, 149
Disable 3DES in TLS, 160
Disabled checkbox, troubleshooting, 247
Disabling digital signatures, 247
DocuSign CA, setting, 77
DocuSign SA
applications that work with DocuSign SA, 12
architecture, 16
components, 12
data flow, 16
documentation, 13
does not respond, troubleshooting, 248
end user platforms, 14
environments supported by DocuSign SA, 12
information, viewing in web-based Console, 208
installation, 28
installing client directly from CD, 105
installing with reduced privileges, 251
setting debug level, 157
shutting down in web-based Console, 199
time and date, setting in web-based Console, 197
turnkey solution, 18
uninstalling client, 108
DocuSign SA Administration MMC
adding a CA, 138, 140
backing up database, 116
capabilities, 116
changing system parameters, 147
disabling a CA, 143
downloading log files, 123
high availability options, 122
managing data replication, 223
monitoring appliance network performance, 132
monitoring appliance performance, 131
obtaining a new license, 133
operations fail, troubleshooting, 248
overview, 114
renewing ChosenSecurity authentication key file, 130
renewing RA authentication key file, 84, 128
renewing subordinate CA certificate, 142
restarting DocuSign SA, 117
restarting DocuSign SA services, 117
restoring the appliance in a Directory Independent environment, 169
restoring the appliance in Active Directory, 168
restoring the appliance in LDAP environment, 169
restoring the appliance, overview, 167
setting CA parameters, 143
starting, 114
synchronizing DocuSign SA with the directory service, 136
system parameters, troubleshooting, 248

uploading software updates, 118
uploading SSL certificate, 121
usage prerequisites, 114
DocuSign SA administrative client
installation overview, 28
installation requirements, 29
installing, 30
uninstalling, 32
DocuSign SA Certificate SN, 147
DocuSign SA Configuration Utility
Admin mode
configuration file operations, 236
creating a configuration file, 236
exporting to a configuration file, 237
exporting to a group policy, 237
group policies operations, 237
opening a configuration file, 236
opening a group policy, 237
usage, 236
CA menu, 233
distributing a client configuration
manual distribution, 239
overview, 238
via configuration files, 238
via distributing software, 239
via group policy, 239
via login scripts, 239
downloading the ROOT certificate, 234
editing parameters, 232
End User mode, 238
File menu, Admin mode, 233
generating an installation report, 234
Help menu, 234
installing the ROOT certificate, 233
introduction, 230
menus, 232
modes of operation, 230
overview, 230
running, 230
setting appliance configuration
appliance installation parameters, 240
overview, 240
performance monitoring parameters, 242
using, 230
DocuSign SA Enterprise
back panel, 38
description, 14
environmental conditions, 40
front panel, 38
physical dimensions, 39
DocuSign SA Enterprise HW 8.0
hardware v8.0 installation, 38
DocuSign SA FIPS
description, 14
DocuSign SA FIPS HW v8.0
front panel, 34
DocuSign SA FIPS HW v8.0
hardware v8.0 installation, 33
DocuSign SA FIPS HW v8.0
back panel, 34
DocuSign SA FIPS HW v8.0
physical dimensions, 34
DocuSign SA FIPS HW v8.0
environmental conditions, 36
DocuSign SA FIPS HW v8.0
certificates compliance, 37
DocuSign SA packages, defining in SCCM, 259
DocuSign Signature Appliances
DocuSign SA Enterprise, 14
DocuSign SA FIPS, 14
monitoring appliance network performance, 132
monitoring performance, 131
obtaining a new license, 133
overview, 14
software installation, 40
DocuSign Signature Appliances HW v8.0
installing, 33
Downloading log files, 123

—E—

Email From Address, 155
Email notifications
configuring, 71
mail server name parameter, 155
Enable Automatic User Logon, 154
Enable Radius AD Attribute, 162
Enable User Counters, 155
End-user machine, deploying client on, 103
Enforce FIPS Approved Algorithms, 159
Enhanced Key Usage Enabled, 146
Enhanced Key Usage Mask, 146
Enrolling users in DocuSign SA, 16
Environmental conditions
DocuSign SA Enterprise, 40
DocuSign SA FIPS, 36
Environments supported by DocuSign SA, 12
Error messages
appliance not in factory settings mode, 244
DocuSign SA IP address is invalid, 243
failed error 51, 243
failed error 52, 243
failed error 54, 243
licensing issues, 246
the snapshot for this publication has become obsolete, 246
Expiration date of license, 210
Expiration variance, certificates, 145
Expired user action, 152

Extended Authentication
devices, 113
parameters, setting, 161
supported modes, 113
Extended Authentication Method, 161
External CA Password, 147
External CA User Name, 147
External CA, automated mode
available WWV CAs, 73
ChosenSecurity, 80
DocuSign CA, 77
overview, 19
SSL proxy settings, 71
synchronizing with DocuSign SA, 140
TSCP, 75
External CA, manual mode, 73
External Certificate Authorities, accessing, 267
External resources, accessing, 266
Comodo, 266
DocuSign CA, 266
DocuSign CA TSCP, 266
external CAs, 267
Symantec, 266
Extractable Keys, 150

—F—

Factory settings mode error message, 244
Factory settings, restoring in web-based Console, 200
Failed
installation, 244
operations in DocuSign SA Administration MMC, 248
FIPS, 23
FIPS box HW v8.0, certificates' compliance, 37
Firmware updates, uploading, 118
Front panel
DocuSign SA Enterprise, 38
DocuSign SA FIPS HW v8.0, 34

—G—

GetBackup, 186
GetEvt, 187
getServerReport, 190
Groups management
adding a group, 178
updating a group, 180
viewing groups list, 177
viewing groups status, 177

—H—

Hardware
restarting, 117
Hardware v8.0
installing DocuSign SA FIPS, 33
Hardware v8.1
installing DocuSign SA Enterprise, 38
High availability
client behavior, 216
data replication, 215
installation overview, 217
installing alternate appliance hardware, 218
installing alternate appliance software, 218
installing an alternate appliance, 218
installing the primary appliance, 217
introduction, 215
managing data replication, 223
managing primary appliance failure, 224
overview, 215
resubscribing an alternate appliance, 228
setting alternate appliance as primary appliance, 224
setting primary appliance as alternate appliance, 227
Subscribed Alternates window, 223
HSM Mode, 161

—I—

Inactivity timeout, clients, 158
Install log, downloading, 123
Installation report, generating, 234
Installing
alternate DocuSign Signature Appliance, 218
alternate DocuSign Signature Appliance hardware, 218
alternate DocuSign Signature Appliance software, 218
ChosenSecurity External CA, 80
command line utilities, 186
DocuSign CA, 77
DocuSign SA administrative client, 28, 30
DocuSign SA as a subordinate CA, 99
DocuSign SA client, 104
DocuSign SA client, centralized installation, 258
DocuSign SA Enterprise hardware v8.1, 38
DocuSign SA FIPS hardware v8.0, 33
DocuSign SA in Active Directory, 41
DocuSign SA in Directory Independent environment, 60
DocuSign SA in LDAP environment, 52
DocuSign SA with reduced privileges, 251
DocuSign Signature Appliances HW v8.0, 33
DocuSign Signature Appliances in a high availability configuration, 217
failed, troubleshooting, 244
internal CA, 69
overview, 28
primary DocuSign Signature Appliance, 217
progress bar, troubleshooting, 245, 246
ROOT certificate, 112
troubleshooting, 243

TSCP External CA, 75
uninstalling the client, 108
uninstalling the DocuSign SA administrative client, 32
Installing DocuSign SA administrative client
installation procedure, 30
requirements, 29
Installing DocuSign SA in Active Directory
installation procedure, 43
overview, 41
permissions, 41
user types, 52
Installing DocuSign SA in Common Criteria EAL4+ mode
installation procedure, 66
Installing DocuSign SA in Directory Independent environment
installation procedure, 60
overview, 60
Installing DocuSign SA in LDAP environment
installation procedure, 53
overview, 52
supported directories, 53
Installing DocuSign SA with reduced privileges
administrating DocuSign SA after the installation, 255
creating a CDP, 257
creating an SCP, 256
installation instructions, 254
introduction, 251
joining DocuSign SA to MS domain, 255
order of operations, 253
overview of regular installation, 252
performing user synchronization, 257
pre-installation action, 253
publishing the ROOT certificate, 257
restoring capabilities, 255
updating userCertificate, 257
Intended audience, 15
Internal CA
installing, 69
installing DocuSign SA as subordinate CA, 99
overview, 18
Internal OTP enabled, 167
Introduction
to digital signatures, 11
to DocuSign SA, 11
to DocuSign SA architecture, 16
Invalid IP address, 243
IP address
failure when setting via the console interface, 243
invalid, 243
setting in Web-based Console, 196

—J—

JWT
JWT Audience, 166
JWT Common Name, 166
JWT Display Name, 166
JWT Email Address, 166
JWT Fetch Additional User Info, 167
JWT Group Name, 166
JWT Groups Member, 167
JWT Issuer, 166
JWT Set Document, 166
JWT Symmetric Key, 166
JWT Telephone Number, 166
JWT UPN, 166
JWT Window, 167
JWT working method, 166
Object Guid, 166
OpenID Discovery Document, 166
JWT Audience, 166
JWT Common Name, 166
JWT Display Name, 166
JWT Email Address, 166
JWT Fetch Additional User Info, 167
JWT Group Name, 166
JWT Groups Member, 167
JWT Issuer, 166
JWT Set Document, 166
JWT Symmetric Key, 166
JWT Telephone Number, 166
JWT tickets, 24
active mode, 26
passive mode, 25
ticket requirements, 26
JWT UPN, 166
JWT Window, 167
JWT Working Method, 166

—K—

Key length for RSA Key pool, 151
Key Usage Mask, 146
Keys
central storage of, 17

—L—

Language support, 102
LDAP
Allow Only Built-in DocuSign SA Admin, 150
Directory Server Search Base, 150
parameters, setting, 156
LDAP Authentication Method, 157
LDAP DocuSign SA user name, 157
LDAP DocuSign SA user password, 157
LDAP environment
installing DocuSign SA software, 52

restoring appliance, 169
supported directories, 53
LDAP Secure mode, 157
LDAP Server Realm name, 157
LDAP Server UID attribute, 157
License
obtaining new, 133
requesting new, 133
uploading new, 134
viewing expiration date, 210
Location, 164
Log files, downloading, 123
Login for Sign Window, 163
Logon prompt
setting, 152
specifying when it appears, 154
viewing in SCP, 111

—M—

Mail Server Name, 155
Mail Server Port, 155
Managing
appliance, 114
Max Password Failed Attempts, 156
Maximum number of rows, 155
Maximum Password Validity, 156
Maximum Repeats in password, 156
Maximum RSA key pool size, 151
Maximum Sequence in password, 156
Microsoft Active Directory
adding ROOT certificates to trusted CA list, 112
Automatic deployment of DocuSign SA client, 258
installing DocuSign SA software, 41
installing DocuSign SA with reduced privileges, 251
multiple trusted Active Directory, 41
parameters, setting, 148
permission considerations, 41
restoring appliance, 168
SCP, 110
Minimum Password Length, 155
Minimum Password Validity, 156
Minimum server TLS version, 160
Modifying system parameters, 147
Monitoring appliance performance, 131
activating monitoring, 131
stopping monitoring, 131
viewing monitoring results, 132
Monitoring network performance, 132
Multi-language support, 102
Multipe, 20, 138
Multiple Active Directory domains deployment, 135
Multiple trusted Active Directory support, 41

—N—

Network monitoring
activating monitoring, 132
stopping monitoring, 133
viewing monitoring results, 133
Network performance monitoring, 132

—O—

OATH TOTP
Internal OTP enabled, 167
OTP length, 167
OTP Validity period, 167
Time to init OTP after reset, 167
Object Guid, 166
One Time Password
Radius server settings, 162
using a Radius Server, 161
One Time Password using an internal OTP mechanism, 161
OpenID Discovery Document, 166
Operating systems supported for client, 103
OTP devices
extended authentication mechanisms, 18
management in Radius Server, 22
recommendations, 24
OTP length, 167
OTP OATH validation window, 163
OTP validation method, 163
OTP Validity period, 167
Outlook, disabling digital signatures, 247
Overview of DocuSign SA, 11

—P—

Password in Directory Independent environment
setting policy, 155
Performance monitoring, 131
Periodic Directory Sync Timer, 150
Permissions in Microsoft Active Directory, 41
Permit upload RSA keys, 151
PKI
DocuSign SA's integrated solution, 18
Primary DocuSign Signature Appliance
installing, 217
overview, 215
setting as alternate appliance, 227
Primary LDAP server address, 156
Primary LDAP server port, 156
Process, 152
Prompt for Logon, 152
Prompt for Signature, 154

—R—

RA certificate
Download RA certificate request, 84, 128

Get an RA certificate, 96
Renew RA certificate, 84, 128
serial number, 147
troubleshooting failed upload, 245
Upload RA certificate reply, 78, 84, 128
Radius callback list in Common Criteria mode, 163
Radius customer AD attribute, 163
Radius Server, 21
OTP Management, 22
Radius Server IP Address, 162
Radius server parameters, setting, 162
Radius Server port, 162
Radius Server Retries, 162
Radius Server Secret, 162
Radius Server Timeout, 162
Refresh timer, certificates, 152
Refresh window, certificates, 145
Refreshing certificates, 141
Regenerate User Key, 151
Rejoin Appliance to Active Directory domain, 136
Report Apps Names to Audit log, 155
Report Signatures to Audit log, 154
Require Static Password Logon, 162
Resetting tamper mechanism in web-based Console, 199
Restart server
command line utility, 188
Restarting
DocuSign SA services, 117
DocuSign Signature Appliance, 117
Restarting appliance in web-based Console, 199
RestartServer.exe, 188
RESTful Web Services Support, 159
Restoring appliance
failed appliance restore, troubleshooting, 249
in a Directory Independent environment, 169
in Active Directory, 168
in LDAP environment, 169
overview, 167
Restoring appliance HW v8.0 FIPS
after hard disk failure, 213
Restoring appliance HW v8.1 Enterprise
after hard disk failure, 212
Restoring factory settings
via the web-based Console, 200
Restoring factory settings for HW v8.0 FIPS
in case of hard disk failure, 213
Restoring factory settings for HW v8.1 Enterprise
in case of hard disk failure, 212
Resync Appliance clock with Active Directory, 135
ROOT certificate
adding to trusted CA list, 112
downloading, using the DocuSign SA Configuration utility, 234
installing, 112
installing using the DocuSign SA Configuration utility, 233

—S—

SAML
Accepting Relying Parties Tickets, 164
SAML Common Name, 164
SAML Display Name, 165
SAML Email Address, 165
SAML Fetch Additional User Info, 165
SAML Group Name, 165
SAML Groups Member, 165
SAML Ignore Revocation Status, 165
SAML Object Guid, 165
SAML PN, 165
SAML Telephone Number, 165
SAML Window, 165
SAML working method, 164
SAML Common Name, 164
SAML Display Name, 165
SAML Email Address, 165
SAML Fetch Additional User Info, 165
SAML Group Name, 165
SAML Groups Member, 165
SAML Ignore Revocation Status, 165
SAML Object Guid, 165
SAML PN, 165
SAML Telephone Number, 165
SAML tickets, 24
active mode, 26
ADFS, 25
passive mode, 25
ticket requirements, 26
SAML Window, 165
SAML Working Method, 164
SCCM automatic client deployment
advertising a task sequence, 264
client installation components, 258
creating a task sequence, 260
defining and advertising task sequence, 259
defining DocuSign SA packages, 259
SCP
in a Microsoft Active Directory, 110
overview, 109
Search Base in LDAP Server, 157
Secondary LDAP server address, 156
Secondary LDAP server port, 156
Server logs, uploading, 207
Server report
downloading, 127
Service Restart operation, 117
SetSCP, 190
Setting IP address
in Web-based Console, 196

Shutting down
DocuSign SA services, 117
DocuSign SA, via the web-based Console, 199
DocuSign Signature Appliance, 117
Signers User Group (AD, 148
SNMP Accepted Community Name, 164
SNMP Manager 1, 164
SNMP Manager 2, 164
SNMP Monitoring
address of the first management system, 164
address of the second management system, 164
contact name of SNMP agent, 164
enabling the SNMP service, 163
location name of SNMP agent, 164
which members can manage the SNMP agent, 164
SNMP Service, 163
Software
installation failed, 244
installing, 40
installing in a Directory Independent environment, 60
installing in Active Directory, 41
installing in LDAP environment, 52
updates, uploading, 118
Software, uploadingg, 206
SSL certificate, uploading, 121
SSL proxy
specifying IP address, 158
specifying password, 158
specifying port number, 158
specifying usage, 158
specifying user name, 158
SSL Proxy IP, 158
SSL Proxy Password, 158
SSL Proxy Port, 158
SSL proxy settings, 71
SSL Proxy User Name, 158
Starting the DocuSign SA Administration MMC, 114
Storage of keys in DocuSign SA, 17
Subordinate CA
installation, 99
introduction, 70
renewing certificate, 142
Support
DocuSign contact information, 243
DocuSign support contact information, 243
Switch to prime appliance
command line utility, 189
Switch2Prim.exe, 189
Synchronization timer, directory, 149
Synchronizing DocuSign SA with external CA in automated mode, 140
Synchronizing DocuSign SA with the directory service, 136
Syslog Server IP Address, 155
System parameters
Accepting Relying Parties Tickets, 164
Add Certificate to CRL, 145
Additional Radius IPs (CC Mode), 163
AIA Publication Location, 144
Allow Get Backup Anonymously, 159
Allow Only Built-in DocuSign SA Admin, 150
Alternate Extended Auth Mode, 161
Alternate Radius Server Address, 162
Alternate Radius Server Port, 162
Appliance Administrator Group, 149
Appliance Debug Level, 157
Appliance RA certificate serial number, 147
Audit log storage period, 155
Automatic Deletion of Users, 148
CA Account Name, 147
CA Cert Hash Algorithm, 145
CA Range, 146
CA Service Connection Point, 146, 147
Case Sensitive Username, 159
Certificate Common Name, 146, 150
Certificate Expiration Variance, 145
Certificate Refresh Timer, 152
Certificate Refresh Window, 145
Certificate Validity Period, 144
Certificate's country, 146
Certificate's organization, 146
Certificate's organizational unit, 146
Clients Inactivity Timeout, 158
Cloud Monitoring, 160
Cloud Monitoring Reporting Type, 160
Cloud Monitoring timer, 161
Cloud Site ID, 160
Common Criteria Mode, 160
Common Criteria Type, 160
Contact Name, 164
CORS domain for REST API, 159
CPS Object ID, 145
CPS URI, 145
Create Computer Keys, 149
Create Group Keys, 149
Create User Key Mode, 151
CRL Publication Location, 144
CRL Publishing Frequency, 145
CRL Validity Period, 145
Default Radius password length, 162
Delete expired users by window, 152
Directory Server Search Base, 150
Directory Synchronization Timer, 149
Disable 3DES in TLS, 160
DocuSign SA Certificate SN, 147
Email From Address, 155
Enable Automatic User Logon, 154

Enable Radius AD attribute, 162
Enable User Counters, 155
Enforce FIPS Approved Algorithms, 159
Enhanced Key Usage Enabled, 146
Enhanced Key usage Mask, 146
Expired user action, 152
Extended Authentication Method, 161
External CA Password, 147
External CA User Name, 147
Extractable Keys, 150
HSM Mode, 161
Internal OTP enabled, 167
JWT Audience, 166
JWT Common Name, 166
JWT Display Name, 166
JWT Email Address, 166
JWT Fetch Additional User Info, 167
JWT Group Name, 166
JWT Groups Member, 167
JWT Issuer, 166
JWT Set Document, 166
JWT Telephone Number, 166
JWT UPN, 166
JWT Window, 167
JWT Working Method, 166
Key length for RSA Key pool, 151
Key usage Mask, 146
LDAP Authentication Method, 157
LDAP DocuSign SA user name, 157
LDAP DocuSign SA user password, 157
LDAP Secure mode, 157
LDAP Server Realm name, 157
LDAP Server UID attribute, 157
Location, 164
Login for Sign Window, 163
Mail Server Name, 155
Mail Server Port, 155
Max password failed attempts, 156
Maximum number of rows, 155
Maximum Password Validity, 156
Maximum Repeats in password, 156
Maximum RSA key pool size, 151
Maximum Sequence in password, 156
Minimum Password Length, 155
Minimum Password Validity, 156
Minimum server TLS version, 160
missing from DocuSign SA Administration MMC, 248
modifying, 147
Object Guid, 166
One Time Password using a Radius Server, 161
One Time Password using an internal OTP mechanism, 161
OpenID Discovery Document, 166
OTP length, 167
OTP OATH validation window, 163
OTP validation method, 163
OTP Validity period, 167
Periodic Directory Sync Timer, 150
Permit upload RSA keys, 151
Primary LDAP server address, 156
Primary LDAP server port, 156
Process Pending Request Timer, 152
Prompt for Logon, 152
Prompt for Signature, 154
Radius customer AD attribute, 163
Radius Server IP Address, 162
Radius Server Port, 162
Radius Server Retries, 162
Radius Server Secret, 162
Radius Server Timeout, 162
Regenerate User Key, 151
Report Apps Names to Audit log, 155
Report Signatures to Audit log, 154
Require Static Password, 162
RESTfulWeb Services Support, 159
SAML Common Name, 164
SAML Display Name, 165
SAML Email Address, 165
SAML Fetch Additional User Info, 165
SAML Group Name, 165
SAML Groups Member, 165
SAML Ignore Revocation Status, 165
SAML Object Guid, 165
SAML Telephone Number, 165
SAML UPN, 165
SAML Window, 165
SAML Working Method, 164
Search Base in LDAP Server, 157
Secondary LDAP server address, 156
Secondary LDAP server port, 156
Signers User Group (AD), 148
SNMP Accepted Community Name, 164
SNMP Manager 1, 164
SNMP Manager 2, 164
SNMP Service, 163
SSL Proxy IP, 158
SSL Proxy Password, 158
SSL Proxy Port, 158
SSL Proxy User Name, 158
Symmetric Key, 166
Syslog Server IP Address, 155
The Locality name, 147
Time to init OTP after reset, 167
Use AIA Location Settings, 144
Use CDP Location Settings, 144
Use SSL Proxy, 158
User Activation, 154

User Certificate Publishing, 150
User Must Change Password, 156
Users Administrator Group, 149
Users Key Length, 151
Web Services Support, 159
System tray icon, 111
Administrator actions, 111
right-click menu options, 111

—T—

Tamper evidence, 23
Tamper mechanism
resetting in web-based Console, 199
Tamper response, 23
Task sequence
advertising in SCCM, 264
creating in SCCM, 260
Terminal server, deploying client on, 103
The Locality name, 147
Time to init OTP after reset, 167
Time, setting in web-based Console, 197
Touch screen of web-based Console, 212
Troubleshooting
administrative problems, 248
alternate DocuSign SA installation, 246
appliance does not start, 246
appliance not in factory settings mode, 244
backup fails, 250
cannot see personal certificates, 247
client-related problems, 247
communicating with DocuSign CA, 245
communicating with TSCP CA, 245
console-related problems, 246
default values do not appear in the directory setup dialog box, 244
DocuSign SA Administration MMC operation fails, 248
DocuSign SA does not respond, 248
DocuSign SA parameters missing from DocuSign SA Administration MMC, 248
installation, 243
installation fails, 244
installation issues, 245
IP address invalid, 243
overview, 243
progress bar during installation, 245
restore operation fails, 249
setting IP address via the console, 243
signatures in Outlook, 247
users do not receive certificates, 249
Trusted CA list, adding ROOT certificates to, 112
TSCP external CA
uploading CA information, 78
TSCP external CA, setting, 75
Turnkey solution, 18

—U—

Uninstalling
DocuSign SA administrative client, 32
DocuSign SA client, 108
Updates, uploading, 118
Upgrading
overview, 118
Uploading updates, 118
Use AIA Location Settings, 144
Use CDP Location Settings, 144
Use SSL Proxy, 158
User
authentication, 17
enrollment, 16
User Activation, 22, 154
User Certificate Publishing, 150
User groups, 148
User Must Change Password, 156
Users Administrator Group, 149
Users do not receive certificates, troubleshooting, 249
Users Key Length, 151
Users Management utility
activating, 171
adding a user, 174
deleting a user, 176
displaying user information, 177
generating a Users report, 173
login, 173
login using built-in administrator, 174
logout, 174
main window, 172
managing groups, 177
menus, 173
overview, 170
resetting a user's password counter, 174
resetting a user's signature counters, 174
resetting signature counters, 173
right-click menu, 184
setting user password, 176
status bar, 173
toolbar, 183
user fields, 172

—V—

Validating signatures
installing ROOT certificate, 112
Viewing
certificates in store, troubleshooting, 247
DocuSign SA information in web-based Console, 208

—W—

Web server, deploying client on, 104
Web Services Support, 159
WinCap copyright notice, 268