Electronic Signatures

Last Modified on 03/26/2020 3:43 pm CDT

Electronic Signatures

E-signatures are unique objects created when an employee signs a document in HRCenter. Signatures can be added to any form and may also require an additional signature by service rep to sign when processing those electronic documents. In this article, we will take a closer look at those signatures and how to inspect them in Enterprise.

For more information on the legality of E-signatures, check out E-Sign Legality.

View a Document E-Signature

To review an e-signature, first navigate to the employee record in Enterprise. Then locate the document you wish to review.

In the example below, we will be looking at an employee's federal I-9:



To open the document, double-click the item. This will open the file in your preferred PDF

viewer. In the lower left-hand corner, you will find the e-signature:



Note The document is signed by the tenant (your company) and the signatures on the document are for the employee and the service rep who reviewed the document.

Checking Validity

You can check the validity of the signature by selecting the signature box with a click of your mouse.

This will open a pop-up window. The box indicates that this document has not been altered since being signed. It also indicates that there have been no changes to the document.

This is a result of the process of having the employee sign followed by having the service rep sign:



By selecting signature properties, you can further explore more details concerning the signature:

Signature Properties

Signati	ure validity is UNKNO	WN.		1		
Details				•		
Signed by:	twdemo			S <u>h</u> ow Cer	tificate	
Reason:	Greg.Matter	norn 2018-10	-01 21:38:48 (I			
Date:	2018/10/01 17:16	:49 -05'00'	Location:	RD2818780B1182	2	
Validity Su	immary					
The	document has not	been modified s	ince this signatu	re was applied.		
The signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities.						
Signing time is from the clock on the signer's computer.						
Sign 201	ature was validated 8/10/01 17:16:49 -	as of the signin 05'00'	g time:			
Signer's Cor	ntact Information:					
When authou that ti signer. the Ce certific	you directly trust a ity, you should cont e signer is who he/ For example, you c rtificate Viewer to v ate.)	signer's certifica act the signer t she reports to t an confirm the riew the MD5 di	te that is not is o verify the cert oe, then verify if certificate's MDS gest, and to imp	sued by a root cer ificate. Once you the certificate is f digest with the s port and directly tr	tificate are confident from the igner. (Use ust the	
					Close	

Choosing 'Show Certificate' will allow you to see the specific certificate paths that belong to the document. Select 'Show Certificate' to continue exploring greater details:

Certificate Path	Trust Revocation				
LWUEID	A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.				
	Use this certificate as a trusted root				
	If signature succeeds, trust this certificate for:				
	Validating Signatures				
	☑ Validating Certified Documents				
	Add to Trusted Certificates				
Show Certificate					
	ОК				

A documents 'Thumbprint' can be viewed by selecting the 'Details' tab. This thumbprint can be used by TempWorks to verify your company:

 \times

👷 Certificate		×
General Details Certification Pat	h	
Show: <all></all>	\checkmark	
Field Subject Public key Public key parameters Authority Key Identifier Subject Key Identifier	Value a 281ec09-a5d0-4eb5-82af-2d RSA (2048 Bits) 05 00 KeyID=8e ba 85 fb 06 0f f0 9 8e ba 85 fb 06 0f f0 95 68 fb	
	23 7e 5f ed e0 73 7d bb b5 cd	
23 7e 5f ed e0 73 7d c9 32 01 4e 10	bb b5 cd 2b e9 0b 24 14	-
	Edit Properties Copy to File	
	ОК	

Related Articles